SCC CCN

Canadian Data Governance Standardization Roadmap

Standards
Council
of Canada

Open a world of possibilities.

Canadä

Table of contents

Acknowledgements

Sincere thanks are extended to all of the individuals and organizations (see Annex E) who provided technical input and/or other support associated with the development of this Roadmap. It is because of their investment, involvement and contributions over the last year that this document has been made possible.

The Roadmap is based on a consensus of those who actively participated in its development and does not necessarily reflect the views of the individuals or organizations who participated in its development.

Also, a sincere thanks to the American National Standards Institute (ANSI), and in particular Jim McCabe, ANSI, Senior Director of Standards Facilitation at ANSI. The roadmap is based on the methodology and mechanisms established by ANSI over the last 15 years. For more information on ANSI's Standardization Collaboratives, please visit their web site: https://www.ansi.org/standards-coordination/coordination-us-system

Funding for this initiative was provided by the Standards Council of Canada in support of Canada's Innovation and Skills Plan to work directly with Canadian innovators to help them leverage the standardization system for their economic growth and competitiveness.

Message from the Co-Chairs of the Data Governance Standardization Collaborative

The Data Governance Standardization Collaborative was established in 2019 as one of the first deliverables that followed the launch of Canada's Digital Charter. When we convened the Collaborative, we challenged ourselves to build a standardization roadmap by the end of 2020. Little did we know how much would change around the world — and how quickly standards would reveal themselves to be the bridge we'd need to help us get to the other side of this global crisis.

The challenges of the COVID-19 pandemic have accelerated fundamental shifts in our society and economy. We live in a world where data come from more sources than ever and move continuously in all directions. And that's why establishing a common language for data-sharing is a critical task.

Standards are essential for collaboration. They are the bridges we use to communicate ideas between individuals, across sectors and nations, even across time. Standards also accelerate innovation. They do the heavy lifting of integrating data and maintaining interoperability of systems, which leaves innovators free to focus on discovery and invention. Standards have been recognized as agile methods of adapting principles-based law to particular sectors and technologies, and as tools to promote future compliance efforts. We've seen a remarkable example of standards in action in the pandemic. Standards are what enabled the unprecedented level of data-sharing around the world that led scientists to develop vaccines against COVID-19 in record time.

The Collaborative has been working hard to find areas of potential collaboration and innovation over the past year. Our working groups convened virtually on case studies that serve as pragmatic examples of the key issues facing data governance today. One study examined data weaknesses in our health-care system. A second took on Consumer-Directed Finance, or "open banking" as it's commonly known. A third looked at how our food gets to our table as the global food supply chain undergoes a digital transformation. We're grateful to the working groups for all the time and thought they put into mapping the standardization landscape. They triaged hundreds of standardization issues down to the thirty-five recommendations you'll find in this initial roadmap.

In order to move these recommendations forward, the next piece of the bridge we need to build is its foundation. Trust in the digital economy will be essential to protect the health, safety and well-being of Canadians. Our Collaborative will continue to engage with policy makers on ways to promote public trust and safeguard Canadians' privacy and security as we work on data-governance issues.

We want to thank our members for collaborating, for trusting each other, and for committing to carry our work forward for the benefit of all Canadians. We also want to express our appreciation for the support and guidance of our founder, the Standards Council of Canada.

Anil Arora, Chief Statistician of Canada

Philip Dawson, Senior Policy Counsel, Responsible AI Institute

Message from the CEO, Standards Council of Canada

The handling and management of data impact the long-term health, well-being and prosperity of Canadians. We have a tremendous opportunity to leverage and use data better in our society to drive growth and keep Canadians safe. Canada's Digital Charter identifies standardization as a tool to support innovation and ensure Canadian companies remain competitive globally.

The Standards Council of Canada (SCC) established the Canadian Data Governance Standardization Collaborative to coordinate data governance standardization strategies across Canada. We set an ambitious workplan. Over the past year, we have collaborated with more than 220 Canadians across government, industry, civil society, Indigenous organizations, academia and standards development organizations to take a hard look at Canada's data governance frameworks — the current state and challenges, and the ideal future state.

The Roadmap that we have developed as a Collaborative describes key issues related to data governance, identifies standardization gaps and provides recommendations on how to close those gaps. This document is meant to guide us through an important moment in our history. It is a tool to help tackle the challenging questions we face when contemplating and planning for the future of data governance in Canada.

It has been no easy feat to develop and finish the Roadmap during a pandemic. I continue to be impressed by the passion that every single participant has brought to the table. The strength of this Collaborative is in the broad range of people who are committing their time and energy to this effort.

Standardization, properly applied, is about highlighting excellence and promoting it. It is about unlocking potential and ensuring that Canadians are getting access to the safest products, systems and technological solutions the world has to offer.

SCC will be looking to implement this Roadmap and its 35 recommendations over the next few years, in close partnership with standards development organizations and other key partners. We will lead this work by doing what we do best: helping to solve complex issues by convening interested parties and the standardization network to co-create the strategies and solutions needed to protect the health and safety of Canadians.

Chantal Guay

Ms. Chantal Guay, ing. P.Eng. FCAE

Executive Summary

In 2019, with the launch of Canada's Digital Charter and its action plan, standards and conformity assessment were highlighted as vital tools for "encouraging development and implementation of new data governance mechanisms." The Digital Charter states that "Canada has an opportunity to be proactive and take a leadership role in emerging areas in digital and data management, helping to establish benchmarks or global standards... . **Allowing for internationally driven certifications and standardizations could bring some certainty to these disruptive markets and allow Canada to help shape global norms."**[1]

In November 2020, the government proposed the Digital Charter Implementation Action with the goal of building a national data strategy to "harness the economic benefits that can flow from data, while also mitigating the potential harms." At the same time, Canada's Industry Strategy Council shared its ambitious growth plan for building a digital, sustainable and innovative economy, highlighting the need for standards and conformity assessment (i.e., standardization) as key tools for Canada to become a **digital and data-driven economy**.[2]

The Canadian Data Governance Standardization Collaborative (DGSC, also known as "the Collaborative") was launched as a response to the Digital Charter **to coordinate the development and compatibility of data governance standards and complementary conformity assessment programs in Canada, contributing to the digital and the data-driven economy**. This Roadmap is the first product of the Collaborative, focused on the data value chain of data governance, describing the current and desired Canadian standardization landscape, including recommendations to address gaps and new areas where Canada can be a standards setter and influencer internationally in the sphere of data governance/big data;

Three broad themes emerge from this Roadmap, based on 35 recommendations from the Collaborative, highlighting the **imperative need for data governance standardization solutions that focus on both operative and strategic needs**:

1. **Quality** — establishing standardization solutions for systems and controls so that high-quality data can be achieved.
2. **Trust** — building the foundation of trust through standardization to know that those using data are using it properly and respecting privacy, security and transparency regulations and frameworks.
3. **Ethics** — Ensuring that AI machine learning tools are ethical and that explainability (can be explained in human terms) can be achieved and supported by standardization, systems and other forms of controls.

Standardization solutions will result in a higher quality of data and trust in access mechanisms, and ensure that tools being deployed are ethical, fair and lawful.

This report builds on the recommendations of the Digital Charter and puts standardization into action as a catalyst for change and a solution to pandemic recovery efforts. The Roadmap provides a framework to ensure that the conversations and interactions involving data among governments, Indigenous governments and organizations, industry, civil society, standardization bodies and Canadian citizens are meaningful, trustworthy and transparent.

[1] Canada's Digital Charter in Action: A Plan by Canadians, for Canadians https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

[2] "The digital economy is the economic activity that results from billions of everyday online connections among people, businesses, devices, data, and processes. The backbone of the digital economy is hyperconnectivity which means growing interconnectedness of people, organisations, and machines that results from the Internet, mobile technology and the internet of things (IoT)." https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html Data-driven economy is when data is used to improve social and economic processes, products, organisational methods and markets. "The data-driven economy, like the knowledge-based economy that spawned it, features economies of scale and network externalities, which give rise to concentrated market structures, expanded economic rents and incentives for strategic behaviour, including in trade policy." https://www.cigionline.org/articles/economics-data-implications-data-driven-economy#:~:text=In%20terms%20of%20market%20structure,including%20in%20trade%20policy%20(as

Standardization is a tool that more traditional sectors are familiar with. Standardization is embedded in our building codes and regulations and are seamlessly used to build our infrastructure in a manner that keeps us safe without having to think about "why" we feel safe. We are now in an era where people, organizations and communities are using or interacting with an intangible infrastructure (i.e., the Internet), yet rules governing, for instance, data privacy and safety are still in their infancy. Standardization, and all that it entails, adopts an approach that acknowledges the need for continuous change and improvement (of standards, of services, of products, etc.), and provides a holistic approach toward auditing and compliance as both strategic and operational data governance issues evolve.

This Roadmap sets the stage for a fulsome discussion about how to action the various components and elements that make up data governance in Canada through standardization. In addition to its broader policy implications, the Roadmap presents concrete recommendations to be implemented over the next five years to achieve the greatest impact while utilizing resources efficiently and effectively.

This Roadmap is your **CALL TO ACTION**:

- For our government partners, this Roadmap will help you understand how participating in the development of standardization solutions will address public policy needs, including incorporation by reference in regulation, and using national conformity assessment schemes to support internal and external trade agreements;
- For our standardization partners, this Roadmap will support the development of new and needed standardization solutions; issues presented in the Roadmap have been scoped to begin or continue with the development of standardization solutions that can help close identified gaps, and position Canada as a leader in the development of new national and international standards and conformity assessment schemes for data governance;
- For our private-sector partners, this Roadmap can cultivate an understanding of how standardization tools can help industry access new markets, scale up and be first to market, comply with emerging regulations, and provide guidance on how to navigate the standardization system, especially for SMEs with limited resources;
- For our partners from civil society organizations, this Roadmap highlights the need for stronger data governance in civil society and to lead by example by demonstrating "an alternative to the current model of unchecked, large-scale data exploitation by many big technology companies."[3]
- For Canadian citizens, this Roadmap will help you understand how standardization, a tool that is already seamlessly incorporated in your day-to-day life, will help build a safer and more secure digital infrastructure founded on quality, trust and ethics as more and more services and transactions go online and we continue to build digital infrastructures that support the health and safety of Canadians.

Lastly, and **this is the value and foundation of the Collaborative, none of this work can move forward without partnerships *among* all stakeholders**. For Canada and Canadians to benefit from a digital and data-driven economy, standardization tools will be a catalyst to:

- take advantage of private/public/civil-society-sector digital solutions to improve the quality of, streamline and modernize Canada's data infrastructure;
- promote the sharing of data among multiple stakeholders from different sectors and produced by private/public/civil-society-sector organizations on trusted data platforms or portals; and
- increase data owners' control and decision power over the ethical sharing and use of their data to address common policy challenges.

If you need more information on how to use this Roadmap or how to get involved, please contact the Standards Council of Canada at info@scc.ca.

[3] Open Society Foundations, Civil Society Organizations and General Data Protection Regulation Compliance, 2020

How to Use this Report

About Standards and Conformity Assessment

A standard is a document that provides a set of agreed-upon rules, guidelines or characteristics for activities or their results. Standards establish accepted practices, technical requirements, and terminologies for diverse fields. They can be mandatory or voluntary and are distinct from Acts, regulations and codes, although standards can be referenced in those legal instruments (see Guidelines for Incorporating Standards by Reference in Regulations to Support Public Policy Objectives[4]).

Conformity assessment is the practice of determining whether a product, service or system meets the requirements of a particular standard.

Standardization is the development and application of standards. It includes: the work of the committees that develop standards; the publication of standards by standards development organizations; the recognition of standards by national standards bodies such as SCC; the application of standards by businesses, suppliers and customers; the verification that products or services conform to applicable standards (conformity assessment); the accreditation of organizations that provide conformity assessment services; and the use of standards and conformity assessment as an element in public policy as well as in international trade.

The Standards Council of Canada (SCC) is Canada's voice on standards and accreditation on the national and international stage. SCC works closely with a vast network of partners to promote the development of effective and efficient standards that protect the health, safety and well-being of Canadians while helping businesses prosper. As Canada's leading accreditation organization, SCC creates market confidence at home and abroad by ensuring that conformity assessment bodies meet the highest national and international standards. SCC advances Canada's interest on the international scene as a member of the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) by connecting thousands of people to global networks and resources, opening a world of possibilities for Canadians and businesses.

[4] https://www.scc.ca/en/about-scc/publications/documents-de-politique/guidelines-for-incorporating-standards-reference-regulations-support-public-policy-objectives

About the Collaborative

The Data Governance Standardization Collaborative, established in 2019, comprised a community of more than 220 Canadian stakeholders from industry, governments, civil society, academia and Standards Development Organizations (SDOs). Their task was to develop a coherent roadmap of existing and needed standards for data governance and to provide implementable recommendations on how codes of practice, certification and standards can be used to adapt principles-based law to particular sectors, activities or technologies, and to make policy frameworks more agile and trusted by Canadians.

Participation in the effort was open to all Canadian stakeholders regardless of their participation in the voluntary standardization system that is overseen by the Standards Council of Canada. The goal was to have balanced representation from key stakeholder groups active in the data governance sphere. Sectors represented in the Collaborative included Aerospace, Communications, Construction, Digital Technologies, Electronics, Energy, Financial Services, Health, Agriculture and Agri-Food, Government Public Services and Retail Services, among others.

Members of the Collaborative who worked on the Roadmap tackled some of the challenging questions regarding standardization and data governance. The strength of the Collaborative was in the broad diversity of people[5] who committed their time and energy to this enterprise.

Reading the Roadmap

The audience for this Roadmap is broad based and includes: the Government of Canada in support of Canada's Digital Charter and data governance in general; standardization bodies looking for guidance on where to focus efforts on data governance standardization development and strategies; Provincial, Territorial and Municipal governments; regulatory/legislative bodies; industry; academia; and the public when looking for guidance and information on what standardization strategies or activities are taking place to address the complex landscape of data governance.

The Roadmap is meant to guide us through some important, current discussions that will impact our future. As a tool, it is designed to help focus resources in terms of participation by stakeholders in the planning and development of standards and related research and development (R&D) activities to the extent R&D needs are identified. It is assumed that those reading the document are directly affected stakeholders who understand the key issues related to data governance and standardization.

The Roadmap is largely a reflection of the subject matter expertise of those who participated in its development. The breadth and depth of the Roadmap can at first seem overwhelming, which is exactly the sentiment the term data governance can evoke when thinking through the complexities. We are all aware that the handling and management of data have implications across our economy — from finance to healthcare, from education to recreation, from manufacturing to retailing. Data is being generated and analyzed and applied in every aspect of our lives. Without clear standards and conformity assessment schemes in place to guide its proper use, the privacy of our citizens and the competitiveness of our economy is at risk.

The first section of the Roadmap provides the policy context to standardization and data governance in Canada. Use cases are introduced to help tell the story of how new and traditional sectors in the digital economy are navigating a complex data governance regime and the impact this has on Canadians economically, competitively and, most importantly, with regard to security. It also provides results from Indigenous engagement on data governance issues, not as a sum of Indigenous perspectives on data governance but on the need for continued engagement of Indigenous groups in the process in order for them to play a greater role in developing and enforcing standards or initiatives for data governance in Canada.

[5] 41% of the Collaborative members are women; 59% are men,

The second section provides a high-level overview of the 35 key issues the Collaborative focused on and the resulting recommendations. This includes the scope of the key issues, the defined needs and examples of how these issues may impact us as individuals or organizations, drawing attention to how the "intangible" of data governance impacts the "tangible" of our lives. It includes 35 high-level recommendations that put a plan into action for a true Canadian Data Governance Framework.

The third section summarizes the recommendations and next steps that will bring the Roadmap from the theoretical realm to a pragmatic one, putting standards and resulting conformity assessment needs into action.

The annexes provide the detailed work of the Collaborative, including the analysis of the working groups (Annexes A and B), the complete Indigenous engagement report (Annex C), the use case reports (Annex D), membership of the DGSC (Annex E), a glossary of acronyms and abbreviations (Annex F), the Methodology for Developing the DGSC Standards Landscape (Annex G), an Overview of SDOs and other Entities Operating in the Data Governance Space (Annex H) and the detailed standardization landscape (Annex I). For those looking for more specific information or the methodology on how the roadmap was developed, this information will be useful.

Standardization and Data Governance in Canada

State of Play

Data governance is a term wide in scope with origins in information management, centring on best practices for data collection, storage, archiving and purging. Common elements of data governance include Collection, Privacy, Usage, Synthesis/Analysis, Control, Publication, Storage and Archiving/ Disposal. However, with the introduction of the Internet in the early 1990s, these terms, and their implications for people, organizations and communities, have been drastically turned on their heads.

Likewise, terms such as privacy and access to information, especially with the rapid evolution of artificial intelligence and machine learning, Internet of Things devices and sensors, have countries around the world quickly developing data strategies to address the tension between data, as a national "resource," and ethical and privacy concerns of people, organizations and communities. Canada is no exception and, while we have been lauded as rich in innovators and innovation, from a data-driven economical point of view Canada's competitiveness has been lagging in a world that is increasingly driven by data.[6]

In May 2019, Innovation, Science and Economic Development Canada (ISED) launched Canada's Digital Charter: Trust in a Digital World. The charter includes 10 draft principles that "will guide the federal government's work, serving as a digital charter for Canadians to help address challenges and leverage Canada's unique talents and strengths to harness the power of digital and data transformation."[7] The Digital Charter has specifically identified standardization as a tool to help support the innovation ecosystem and ensure Canadian companies remain competitive globally.

Consequently, the Data Governance Standardization Collaborative was established in the summer of 2019 as a cross-sector coordinating body with the objective of accelerating the development of industry-wide data governance standards and specifications that are consistent with stakeholder needs and facilitating the growth of data governance capabilities in line with national and global priorities.

[6] https://ppforum.ca/publications/two-mountains-to-climb-canadas-twin-deficits-and-how-to-scale-them/
[7] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

With the understanding that parallel processes unrelated to voluntary standardization concerning data governance are taking place, the objectives of the Collaborative were to:

- Identify and scope Canadian priority areas for data governance that might benefit from standardization;
- Deliver a comprehensive roadmap describing the current and desired Canadian data governance standardization landscape, including recommendations to address gaps and new areas where standards and conformity assessment are needed; and
- Recommend proposals for national and international standardization initiatives, timelines and organizations that can perform the work.

Activities of the Collaborative were framed under four broad domains (working groups) that used a data lifecycle/value chain model: (1) Foundations of Data Governance, (2) Data Collection, Organization and Grading, (3) Data Access, Sharing and Retention, and (4) Data Analytics, Solutions and Commercialization. Within those domains, broad topical areas of relevance to standards and conformity assessment programs for data governance were identified.

The Collaborative recognizes that a number of standards development organizations and/or similar organizations — nationally, regionally and internationally — are engaged in producing voluntary consensus standards for a wide range of issues related to data governance in order to meet the needs of different industries. The existence of these parallel standards-setting activities only increases the need for Canadian leadership and coordination to maintain a consistent, harmonized and non-contradictory set of data governance standards for use by Canadian stakeholders.

Intangible assets, such as data analytics, are key in today's landscape of information and communication technologies. The role of ownership and commercialization of intangible assets has fundamentally transformed the rules of engagement for economies that hope to prosper in the modern technological environment. As data has grown to be the foundational part of existing industries, as well as a critical part of a growing artificial intelligence industry, the need for governance and protocols has expanded to address new areas of data analytics. Furthermore, these new developments and linkages have tasked regulatory frameworks and subsequent compliance schemes (existing and forthcoming).

Organizations have a growing responsibility in managing the data they produce, as well as the type of analysis they conduct. There is also a growing industry of companies that solely work on external data sets and facilitate data analytics and data management for other organizations. Further considerations need to be made for industry-specific needs, such as highly regulated health and finance sectors, and new needs created by growth in traditional sectors of agriculture and insurance, among others. Companies within each of these areas must address not only how their data is governed within their structure but also how their data interchanges with other companies and organizations.

Ethical considerations for data governance also need to be civil society specific, and this role will need to have a defined space as regulations, best practices and standards are developed. In the paper *Information Ethics: Coalition building with Civil Society and Taking Responsibility for AI Evolution*,[8] the role of civil society in the elaboration of a normative framework is explored. It proposes that "representative regulatory innovation processes must guarantee the capacity of civil society to be active members in policy innovation consultations. Public/private partnerships must become Public/Private/Civil partnerships." The exploitation of personal and community data has also come into mainstream conversations, with discussions on surveillance capitalism and the undermining of personal autonomy and democracy.

[8] Goddard, Valentine and Myriam Côté, Information Ethics: Coalition Building with Civil Society and Taking Responsibility for AI Evolution

The nature of data and its increasing movement across organizations has led to the need to develop and adopt standards to address how data is structured, governed and made secure. Standards development organizations have recently been turning their attention to developing standards to address such needs. Standards for data governance grow from previous standardization requirements for information management, which has evolved to address the needs for data management under industrial automation. In addition to standards development organizations, industry-led consortia and open-source platforms also continue to play a role in information and communication technology standards and include data governance in their scopes.

The sheer volume of standards being developed to support digital strategies is cause for concern. How can we reap the benefits of a digital economy and take into account the health and safety of people, organization and communities when the magnitude of standards being developed in both open and voluntary standardization forums further contribute to the confusion rather than providing clarity? A thoughtful and deliberate understanding of the standardization landscape for data governance needs to be taken into consideration as governments, industry and civil society work to develop data governance frameworks that rely on standards, making up the backbone of data governance frameworks.

Countries and regions are looking at their own data strategies and at the standard and conformity assessment tools they can use to support frameworks for action on data. For example, in September 2020, the United Kingdom shared its National Data Strategy with the goal to "cooperate with nations to develop shared standards that align with the UK's national interests and objectives [where] technical standards are increasingly expressions of ethical and societal values, as well as industry best practice."[9]

In 2020, the European Commission set out a proposal for a Regulation on European data governance (Data Governance Act), which is the first set of measures announced under the 2020 European Strategy for data. One task formulated in the proposal is to "advise the Commission on the prioritisation of cross-sector standards to be used and developed for data use and cross-sector data sharing, cross-sectoral comparison and exchange of best practices with regards to sectoral requirements for security, access procedures, while taking into account sector-specific standardisations activities [... and] to assist the Commission in enhancing the interoperability of data as well as data sharing services between different sectors and domains, building on existing European, international or national standards."[10] In April 2021, the European Commission released a proposal for a new EU AI Regulation, which, as currently formulated, would rely increasingly on standardization and conformity assessments to help ensure data and AI systems are used and managed in ways that protect health, safety and fundamental rights.

The creation of the General Data Protection Regulation (GDPR) has modernized the legal landscape for data privacy on a global scale, causing companies in other parts of the world to quickly understand, adopt and implement data privacy requirements and programs so they can operate within the EU. In support of this, SCC published a guidance document to introduce Canadian organizations to the GDPR[11] with recommended standardization strategies that can facilitate the compliance process. In 2020, the U.S. National Institute of Standards and Technology (NIST) also published a set of guidelines to help U.S. enterprises adapt to increasingly demanding data privacy requirements. The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management is a voluntary set of procedures, which can assist companies to understand the compliance measures with different data protection regulations across the world.

[9] https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#fnref:23

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

[11] https://www.scc.ca/en/about-scc/publications/general/understanding-gdpr-role-standards-compliance

Over the past year, data "has been a lifeline during the global coronavirus pandemic,"[12] and standardization on national, regional and international levels has been leveraged to improve the use of data to innovate and support economic growth. At the same time, standardization, as a public policy tool, is also looking to support fundamental ethical questions around the sharing, use and ownership of data and what this means to individuals as well as to communities.

COVID-19 has accelerated fundamental shifts in our society and economy. We live in a world where data comes from more sources and moves continuously in all directions. Establishing a common language for data sharing is a critical task. Standards are at the centre of this challenge and essential for collaboration. They are the bridges we use to communicate ideas between individuals, across sectors and nations, even across time. If it were not for the standards that governments, academics and businesses agreed upon when building the Internet, this exchange of ideas could not have happened. Standards not only enable us to collaborate, they also accelerate innovation. The most striking example of how standards enable innovation is one that we are all benefiting from: the COVID-19 vaccine.

In the case of COVID-19, standards enabled an unprecedented level of data sharing by scientists around the world, which led to the new coronavirus being sequenced within days of it being identified in China. Less than a year later, we had the first authorized vaccines in Canada. That is the fastest vaccine ever developed, with the previous record held by the mumps vaccine, which took four years. While the research that helped to develop the COVID-19 vaccines started years before, global efforts to share data led to rapid advances that will almost certainly change the future of vaccine science. None of this would have been possible without standards to enable the interoperability and integration of systems to share information[13]. Without standards, we would not have a common language to advance the knowledge generated by research.

Tackling the Challenges and Identifying the Opportunities

Working groups across the Collaborative met virtually a dozen times, collaborating on key data governance issues and use case studies that serve as pragmatic examples facing data governance today.

The working groups have been instrumental in identifying areas where standards already exist, so we can dig into our toolbox and start identifying solutions. Some international standards could be adapted to a Canadian context, but other issues will require real Canadian leadership to ensure that Canada is a standards maker, as well as leader in development of conformity assessment schemes that could be the bedrock of future international accreditation programs, supporting international trade in the intangible economy. For example, SCC, with support and funding from ISED, is facilitating the development of normative type documents for a project on digital credentials. SCC will be introducing conformity assessment criteria and an accreditation program to move this initiative forward and pilot it with Canadian regulators, businesses and conformity assessment bodies.

In order to move the recommendations of this Roadmap forward, we need to foster trust in data-sharing arrangements among governments, industry and civil society groups as information travels among them. As a confederation based on decentralized powers to provinces and territories, Canada exists in a patchwork of regulations. In this context, a standard can serve as a "soft law" that is more digestible, easier to conform to, and applicable from one jurisdiction to another. It is important that the Collaborative continues to engage with policymakers, industry and civil society on ways to promote public trust and safeguard the privacy of Canadians.

[12] http://data.parliament.uk/DepositedPapers/Files/DEP2020-0521/UK_National_Data_Strategy.pdf

[13] https://www.who.int/news-room/feature-stories/detail/standardization-of-vaccines-for-coronavirus-disease-covid-19

This trust is the foundation on which our digital and data-driven economy and society will be built. We need to support not only the development of new standards but also public policies and new legislations. Standardization, properly applied, is about highlighting excellence and promoting it. It is about unlocking potential and ensuring that Canadians are not just getting access to, but are the innovators of the best and safest products, systems and technological solutions the world has to offer — all while ensuring that Canadians encounter fewer barriers to accessing markets.

Use Cases: Setting the Context for Data Governance in Canada

With abstract concepts such as data governance and the role standardization can play in collecting, sharing and using data, it can be challenging to understand the impact or relate to it from an every-day perspective, especially given that data is an intangible asset. To help stakeholders understand the role standardization can have in supporting data governance and trust, three use cases were selected as relatable examples or stories. The use cases focus on Community Health Data; Digital Identity and Open Banking; and Consumer Empowerment and Safety: Digital Food Supply Chains.

In the age of COVID-19, these use cases became even more prevalent to every stakeholder category in Canada because they impacted people and organizations personally, economically and politically.

The first use case on Community Health Data examined data weaknesses in our health-care system. With so many Canadians turning to virtual health care over the past ten months, the need for secure and efficient tools to move data around suddenly became urgent. Statistics Canada came up against this very problem early in the pandemic. The distribution of personal protective equipment to health-care workers was hampered by a lack of standardized coding for equipment across health regions. Canada could deliver equipment, but it could not specify exactly what type was needed. Those are examples of how standardization forms part of the bedrock that life-saving work can rely on.

Recent increases in virtual health care delivery due to the pandemic have also called into question the need for secure and efficient tools that enable interoperability of health data. There are numerous ways in which Canadian communities access health care; the coordination of data is increasingly becoming essential as health is delivered by multiple, independent organizations which, without proper protocols, can weaken the end-to-end supply chain. When the system is not interoperable, the value of that health data weakens, resulting in poor policy and decision making and inhibiting rapid response and innovation. This use case looked at how standardization may help support the implementation of a Canadian Community Health framework, reflecting the values and health needs of Canadians.

The second case study looked at Consumer-Directed Finance, or “open banking” as it is commonly known. With in-person interactions restricted during the pandemic, Canadians are wanting to bank and shop in a digital context wherever possible. It is physically safer to pull out a digital wallet than to hand over a credit card right now. These needs have been driving institutions and governments towards third-party arrangements. But there is a lack of regulation and standards to support this new sector, and a lack of tools such as digital identification to enable it.

That is leaving Canadians behind — economically, competitively and, most importantly, with regard to the security of their data. Canadians need to know their digital credentials will not be sold or hacked. And small businesses need to know that governments are behind them, with e-commerce standards that create a level playing field so consumers feel protected.

Learnings from the Use cases

In the summer of 2020, the DGSC established the Use Case Working Groups consisting of a small group of experts who met 5-6 times to determine applicability of the broader Roadmap issues to their various sectors. The intent of the use cases was not to design standards or propose guidelines but rather to clarify the gaps in support of the Roadmap. Each use case examined different aspects of data governance relevant to specific sectors.

The Consumer Safety group discussed multiple information storage systems utilized across the entire value chain of fresh produce for traceability, allowing for the exploration of data ownership and confidentiality in the areas of:

- data sharing;
- interoperability;
- user rights and credentials;
- ethical usage;
- data quality and analytics; and,
- Artificial Intelligence (AI) and machine learning.

The Open Banking and Digital ID use case took a user-centric focus to explore themes such as:

- requirements for identity verification and authentication — with consideration for individuals who experience difficulties proving their identity or accessing online services;
- data ownership, access and privacy;
- security protocols for sharing client data (i.e., API standards);
- operational guidelines for implementation and adoption risks; and,
- client experience guidelines that reflect values of inclusion, transparency and trust.

A third case study looked at how our food gets to our tables. The global food supply chain has been undergoing a digital transformation. This development holds promise. It can speed up decision making and result in healthier, safer and more efficient outcomes. But data governance standards are needed to ensure that it is done right and that consumers can make informed choices about what they eat. Likewise, the agri-food sector needs guarantees that its supply chains remain quality driven and controlled all the way, including with strong government oversight of the whole farm-to-table process.

The use cases allowed the Collaborative to explore how to best leverage the power of data to the benefit of consumers, governments and industry. Questions were asked as to how trust and transparency in digital technologies could accelerate decision-making processes and drive healthier, safer and economic-based outcomes. Supply chain data governance standardization could enable consumers to make informed choices for their families; governments could develop better oversight programs; industry could ensure the quality of their products; and supply chains could respond more quickly to mitigate and address risks.

The Community Health use case group took a top-down view of the key issues for data governance. The group was inspired by the work of Statistics Canada establishing its CODAS platform (to collect data from multiple sources and render it available for StatsCan and external use) and CIHI's Health Data and Information Governance and Capability Framework (https://www.cihi.ca/en/health-data-and-information-governance-and-capability-framework). During the lifecycle discussions, several recurring challenges were identified and categorized into themes for community health data, such as:

- the benefits of standardization when collecting and coding data at point of origin;
- how data exchange and interoperability assists with the aggregation of data; and,
- how guidance on analytics and insights that includes ethics and transparency can drive action.

Each working group shared their perspectives on the challenges facing their sectors in Canada. All three working groups recommended the need to take quick action, building on what has already been done and ensuring Canada does not fall further behind.

To discuss the impacts of the use cases on the Canadian population, a national consultation occurred between December 2020 and January 2021. The consultations provided opportunities to check in with Canadians on the development of the Roadmap with the goal of building a brand and creating trust with stakeholders regarding standardization and data governance.

More than 160 people took part in the nine sessions that were held (six in English, three in French), including representatives from data security companies, medical and healthcare associations and agencies, financial institutions, third-party service providers, agri-food/agriculture, technology industries, government and regulatory organizations, and strategic advisers.

Participants discussed the **current state** of digital data capture and use for their respective areas of interest in digital identity, health data, open banking and digital food supply chains.

Subsequently, they discussed what they see as the **ideal future state** for digital data capture in these areas. Horizontal issues that were common in all three use cases included Security and Privacy, Interoperability and Standardization, Governance and Regulatory Oversight, and Education.

Below are the high-level recommendations and considerations stemming from the discussion and analysis of the use cases; these recommendations will need to be incorporated into the action plan for the Roadmap in Phase II as standardization solutions are implemented.

SECURITY, PRIVACY AND TRANSPARENCY

Current state: Trust in the security and privacy of digital data was a recurrent theme in all of the dialogue sessions, with participants stressing that earning and maintaining the confidence of consumers will be essential for any system to be successful. People need to know what personal data will be collected and kept, for how long and for what purpose, and they need to feel confident they are not sharing more information than is absolutely necessary to access services. It was noted, for example, that it can be difficult to implement privacy standards for health data and that existing rules do not make it easy for patients to give their informed consent for the sharing and use of their personal health information or clearly identify who owns their data if they become incapacitated or die.

Ideal future state: There was universal agreement that strong privacy protections are needed to minimize the risk of personal information being overshared, mishandled or otherwise compromised, to make data tamper proof, and to ensure the integrity and security of data storage. People must be aware of how their information will be shared and with whom and have greater control over who can access their personal data. The definition of "informed consent" should be clarified and made easier to understand by using plain language. For example, patients should be able to access or share their personal health records, but this requires a fundamental paradigm shift from institutional data ownership and control to a more transparent and democratic consumer-centric model.

INTEROPERABILITY AND STANDARDIZATION

Current state: A key factor in the current lack of interoperability of digital data systems is the broad range of actors and regulators in each of the sectors that were discussed. Participants noted that provincial governments have oversight of digital ID and that existing rules governing data vary in each of the provinces and territories, which can complicate sharing of information between jurisdictions.
For example, the diversity and complexity of the agri-food and agriculture industry means there are significant differences across sectors and jurisdictions in Canada, and internationally.

These differences result in a lack of integration among health care providers, including the creation and storage of segregated information, fragmentation and suboptimal cooperation in the banking sector, and data silos in the food industry that limit the transfer of information among numerous sources in the food chain. There is a lack of data and terminology standards within Canada's health system, including when capturing health data. Not enough is being done by the agri-food and agriculture sector to improve the breadth and quality of data available, leading to persistent gaps in food traceability that make it difficult for consumers to easily find information about the origins and production methods of their food.

Ideal future state: There should be increased standardization of data rules to facilitate greater interoperability across the country. This would allow health data to move seamlessly between systems, jurisdictions, providers and patients so people can receive equitable care wherever they live in Canada. It would also give consumers the information they need to make educated food-buying decisions and encourage greater innovation and information sharing across sectors and jurisdictions within the food supply chain. For this to work, however, there must be much greater digitization of information and less reliance on paper-based systems. Participants noted that broad participation is a prerequisite for interoperability to be realized.

GOVERNANCE AND REGULATORY OVERSIGHT

Current state: Although Canada's legal framework regarding privacy is robust, giving the country one of the highest standards of consent in the world, it was noted that consent processes are often too complex and technical for the average person to understand to be able to make an informed decision when sharing their health or financial data. There are also significant differences in provincial and territorial laws restricting health data linkages and no laws to enable open banking in Canada. Participants mentioned that Canada is falling behind other countries in developing the necessary legal and regulatory frameworks governing digital data.

Ideal future state: Interoperability is not just about standardization and common technology but also about the system of laws and regulations governing digital data. Participants stressed the need for effective governance and oversight, along with consistent rules, regulations and standards that are aligned across jurisdictions. Not only will this enable ease of adoption and access to data for everyone, it will also help to create new and enhanced datasets.

EDUCATION

Current state: A lack of consumer awareness was seen as a challenge in each of the topics discussed in the dialogue sessions. Participants in the community health data sessions said most patients and health-care professionals do not have a sufficient understanding of the existing rules governing health data in Canada. Those in the food supply chains sessions said there is no clear value proposition for supply chain participants to accept and take part in a digital food supply chain and that producers may not have the technical knowledge and skills to bring together the data that is being collected so it can be shared across the whole value chain. Digital ID and open banking participants called for governments and industry to work together to ensure that individuals are aware and confident in open banking.

Ideal future state: Participants in the health data dialogue sessions said patients and health-care professionals need more education and awareness about current and future health data rules. Those in the digital ID and open banking sessions agreed that education will be key to making a consumer-centric model — where individuals own and control their data — a reality and help consumers understand what digital ID is and how it impacts them. Participants in the food supply chain sessions said producers and suppliers need a better understanding of how they can contribute to a digital food supply chain, greater access to the necessary technology, and incentives or cost-recovery schemes to encourage buy-in and participation.

The DGSC continues to receive requests for future data governance use cases that could be part of a version two of this Roadmap. For example, a preliminary discussion was held on Children's Surveillance and e-Learning Systems and the need for continued vertical discussions on data governance as it impacts different sectors, particularly as the COVID-19 pandemic has exposed weaknesses in the area of online surveillance as Canadian children adapt and are on-boarded to e-Learning systems (see Annex D for the preliminary consultation report). Based on these discussions, it is clear that future use case could champion best practices for the provision of physical security and cybersecurity services and countermeasures to make Canada a more digitally secure country.

Indigenous Data Sovereignty

The Standards Council of Canada retained Firelight to support the design, development, administration, virtual logistics and facilitation of initial Indigenous engagement across Canada. The objective of this initial engagement is to add Indigenous perspectives on data governance in Canada into considerations for the DGSC Roadmap. Engagement activities included an online survey and key participant interviews. This report provides background on issues related to Indigenous data governance and sovereignty, summarises the results of engagements, and provides a number of recommendations based on input provided by participants. Participants gave consent to use their input in this report prior to survey or interview completion.

Indigenous peoples, like all populations, require high-quality data about citizens, communities, lands, resources and culture to support evidence-based decision making. Yet Indigenous peoples and their governing bodies continue to struggle to gain autonomy over data governance activities. Historically and currently, the collection and management of data about Indigenous communities is largely administered by external bodies, lacking Indigenous leadership and not reflective of the priorities, needs, worldviews and values of Indigenous communities. This has led to the extraction of data from communities, use of inappropriate indicators to measure health and well-being, and misuse of data about Indigenous peoples. It is within this context that Indigenous data sovereignty is emerging — the right of an Indigenous governing body to govern the collection, ownership, dissemination and application of its own data about its communities, members, lands and resources. Indigenous data represents a significant feature of Indigenous sovereignty as a whole and a movement toward self-governance, self-determination and decolonization.

An online survey was selected as a means of engagement in order to reach as broad a group as possible within the engagement timeline. The online survey sought input from participants on the nature and importance of the 10 issues identified by Working Group 1 within an Indigenous context. The online survey was launched, in both English and French, on January 12, 2021 and closed on February 2, 2021. A total of 36 people completed the survey. Participants were asked to rate the importance of each of the 10 Foundations of Data Governance issues. Guidance on trustworthiness, ethical and societal use of data, accountability frameworks and data management governance were most frequently ranked by participants as being very important issues to focus on when developing data governance standards. None of the issues was ranked as not important. Results of the survey are outlined in Annex C, Section 4.1.

Key participant interviews took place with practitioners and experts in Indigenous data governance in order to gain a more in-depth understanding of Indigenous perspectives on these issues. Interview participants were identified based on their expertise and experience working with organizations and/or on projects and initiatives that focus on Indigenous data governance issues. Firelight endeavoured to interview key participants from across Canada with expertise across the unique data governance landscapes of First Nations, Inuit, and Métis communities. Approximately half of those invited to complete an interview were able or willing to participate. A total of 12 interviewees contributed as part of eight key participant interviews. Annex C, section 3.3 provides an overview of key interview participants.

A number of key Indigenous data governance issues were identified upon thematic analysis of survey and interview responses:

- Recognition of Authority: The lack of recognition of the authority of Indigenous governments as sovereign decision makers over all aspects of the lifecycle of data relating to their populations.
- Capacity: The capacity of Indigenous governments and organizations to govern the collection, management, storage and sharing of data. Capacity was described in terms of infrastructure, equipment, human resources, training, technology and funding.
- Access to Data: Indigenous governments and organizations often do not have access to necessary information about the populations they serve. With information housed by researchers, government and other organizations, Indigenous decision makers lack the necessary information to govern.
- Culturally Appropriate Data: Data collection needs to be led by Indigenous organizations, and data collection and management methods need to be reflective of the unique Indigenous cultural context, values and norms relevant to each undertaking.

This report can be used as an initial account of perspectives on Indigenous data governance issues as well as potential means to tackle these issues, but there are a number of limitations to the report that require consideration in interpreting the results. A limited number of participants from Inuit and Métis organizations contributed to the engagements conducted. Due to limitations of time and budget, detailed engagement on each of the 35 issues identified by the DGSC working groups was not possible. The limitations of this report are discussed further in Annex C, Section 1.3.

- A number of existing standards and initiatives were highlighted by participants that are of direct relevance to the potential development of data governance standards. These initiatives all assert the sovereignty of Indigenous peoples to control all aspects of the collection, management and use of data. These are profiled in Annex C, Section 4.3 and include the OCAP® standard, the National Inuit Strategy on Research (NISR) and the First Nations Data Governance Strategy (FNDGS).

A number of recommendations are provided in Annex C, Section 5 based on the input provided during engagements and relating to the continued engagement and participation of Indigenous groups in the DGSC process.

1. Additional engagement of Inuit and Métis organizations and data governance experts is required. Due to limited participation of Inuit and Métis practitioners and experts in engagements, further work is required in order to capture the perspectives of these key Indigenous groups on data governance issues and on the work of the DGSC.
2. Further involvement of Indigenous groups in the DGSC process will be necessary in order to dedicate the time and resources necessary for clearly defining issues brought forward by Indigenous groups and integrating them, where appropriate, into issues already defined by DGSC working groups. This may also include participation of Indigenous representatives in DGSC working groups. For example, based on their high ranking in survey results, a number of key issues from Working Group 1, including Guidance on Trustworthiness, Ethical and Societal use of Data, Accountability Framework, and Data Management Governance will require further input from Indigenous groups.
3. Identifying key Indigenous organizations (including those already developing standards, such as Inuit Tapiriit Kanatami and the First Nations Information Governance Centre) to participate in further phases of DGSC work, including standards development, will be a necessary outcome of further engagements.

Issues and Recommendations

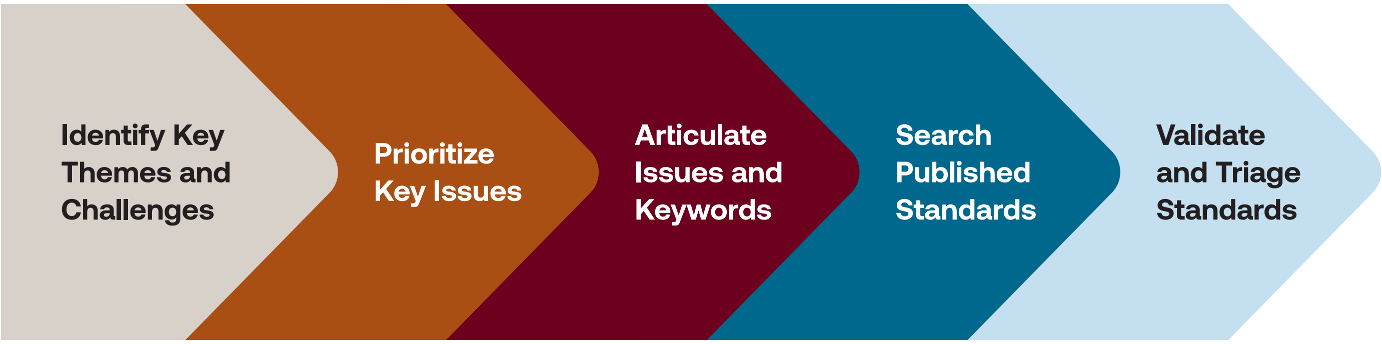
Identification of Key Issues

In January 2020, priority areas for the Roadmap were scoped to 35 issues with the understanding that the Roadmap would not be able to deal with all issues related to the complexities of data governance. Understanding the relevance of standards to data governance was a major undertaking given the breadth of the topics and the magnitude of challenges posed by new technologies along the data supply chain and governance lifecycle.

In the course of a year, working groups held online meetings to describe and scope the chosen issues, inventory existing standards, conduct the gap analysis and draft the Roadmap. Consequently, a participatory research methodology was adopted. The methodology enabled all working group members to be involved as subject matter experts and bring their perspectives into the knowledge-production process (i.e., the development of the Roadmap).[14] Specifically, each working group followed the steps below to map the landscape of published standards relevant to each issue:

[14] Bergold, J., & Thomas, S. (2012). Participatory research methods: A methodological approach in motion. *Historical Social Research/ Historische Sozialforschung*, 191-222.

Diagram 1: Development of Standardization Landscape


Identify Key Themes and Challenges
Prioritize Key Issues
Articulate Issues and Keywords
Search Published Standards
Validate and Triage Standards

In total, about 12,000 standards were identified across the 35 issues (detailed selection methodology can be found in Annex G).[15] The next step was to validate and triage the standards and to share the results with corresponding standards development organizations for their input and validation. National and international standards development organizations were also asked to provide a list of standards under development that may address the 35 identified issues.

Based on the list of standards, the working groups executed a gap analysis of existing and needed standards, specifications and conformity assessment programs for each issue. A "gap" was defined as meaning that no published standard, specification or other type of document exists that covers the issue in question. Each gap was assessed and ranked from a sequencing and timeframes perspective: high (0-2 years), medium (2-5 years), and low (5+ years). As a result, a proposed Roadmap (Diagram 3 at the end of the Recommendations section) was confirmed by working group co-chairs with suggested implementation activities.

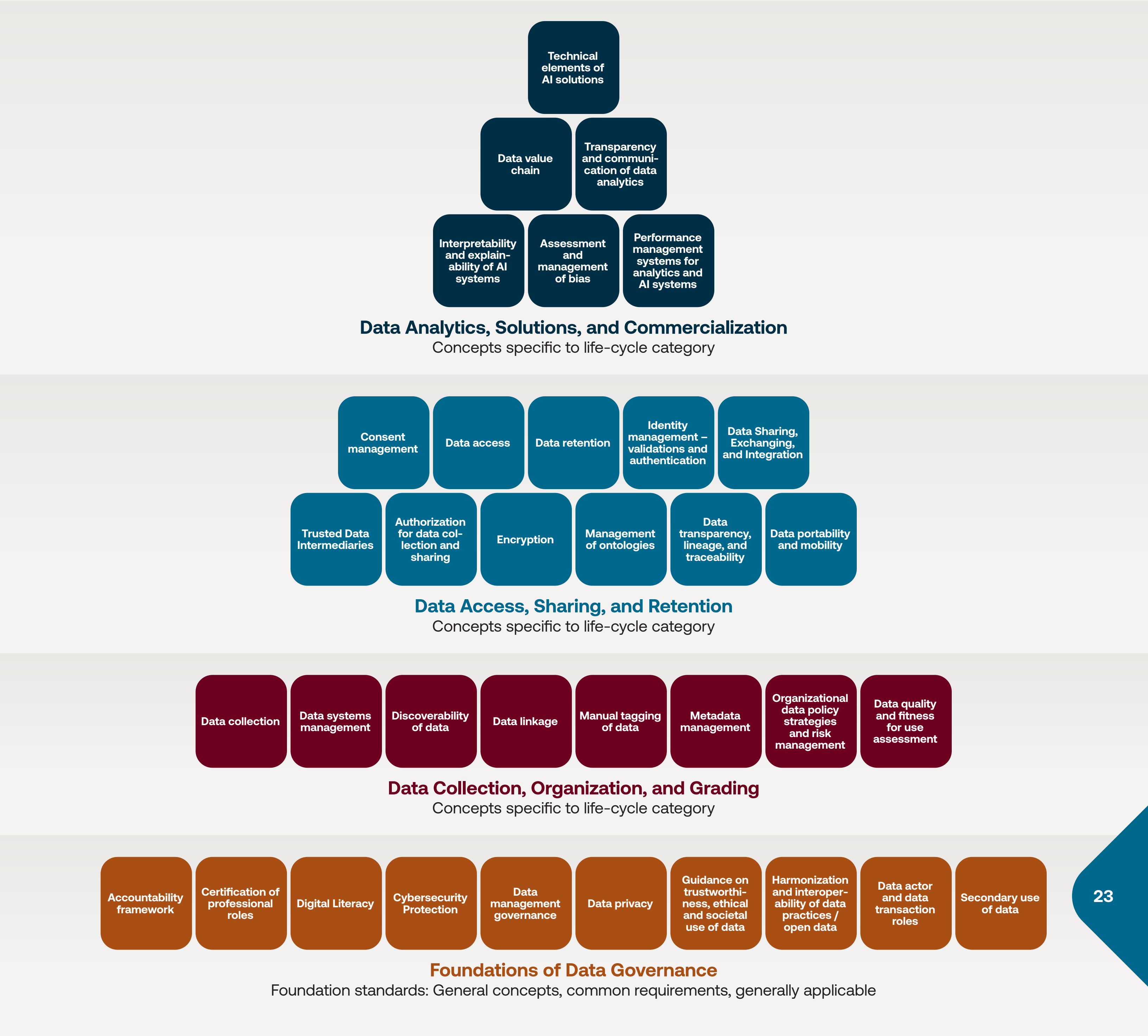
The Roadmap is supplemented by the *DGSC Landscape*, a table of standards that are directly or peripherally related to the issues described in the Roadmap. This can be found in Annex I.

As previously stated, the Roadmap tackles the issues from a lifecycle approach to data which is complex and dynamic, undergoing continual evolution and adaption, and with many parties involved. It was acknowledged from the start that data governance could be examined from many different perspectives and models.

For this purpose, activities were framed under four broad domains and subsequently divided into four working groups: (1) Foundations of Data Governance, (2) Data Collection, Organization and Grading, (3) Data Access, Sharing and Retention, and (4) Data Analytics, Solutions and Commercialization. Within those domains, broad topical areas of relevance to standards and conformity assessment programs for data governance were identified as illustrated in the figure below.

[15] Original search of the 500+ keywords generated about 25,000 standards, more than half of which were removed as a result of duplication.

Diagram 2: Domains and Key Issues of Data Governance



Technical elements of AI solutions

Data value chain

Transparency and communication of data analytics

Interpretability and explainability of AI systems

Assessment and management of bias

Performance management systems for analytics and AI systems

Data Analytics, Solutions, and Commercialization

Concepts specific to life-cycle category

Consent management

Data access

Data retention

Identity management – validations and authentication

Data Sharing, Exchanging, and Integration

Trusted Data Intermediaries

Authorization for data collection and sharing

Encryption

Management of ontologies

Data transparency, lineage, and traceability

Data portability and mobility

Data Access, Sharing, and Retention

Concepts specific to life-cycle category

Data collection

Data systems management

Discoverability of data

Data linkage

Manual tagging of data

Metadata management

Organizational data policy strategies and risk management

Data quality and fitness for use assessment

Data Collection, Organization, and Grading

Concepts specific to life-cycle category

Accountability framework

Certification of professional roles

Digital Literacy

Cybersecurity Protection

Data management governance

Data privacy

Guidance on trustworthiness, ethical and societal use of data

Harmonization and interoperability of data practices / open data

Data actor and data transaction roles

Secondary use of data

Foundations of Data Governance

Foundation standards: General concepts, common requirements, generally applicable

Recommendations

A summary of the recommendations related to the 35 Issues examined is presented, including user stories to help contextualize the issues and to illustrate the impact on us as individuals or organizations. Recommendations are meant to guide future discussion for closing identified gaps, and show how standardization can increase confidence and trust, ensuring Canadians are leaders in developing the safest products, systems and technologic solutions the world has to offer. The summary is not conclusive and should be read in parallel with Annex A that contains the more fulsome discussion of the key issues. When it is time to develop the action plans to implement each recommendation, a starting point will be to read each issue in parallel with use case and Indigenous Engagement reports (Annexes D and C), as well as the standardization landscape (Annex I). A shortened version of the landscape, with a list of directly relevant standards and other normative type documents, can be found in Annex B.

Working Group 1: Foundations of Data Governance

Issue 1 — Accountability Framework

Scope: The liability and control structure for all data collected and created, including roles, responsibilities and accountability of data transactions, including the responsibility of data rights holders, the implication of ownership transfers, the notion of consent, compliance and accountability through regulations.

User story: As a Canadian parent with children in an E-learning environment, I need transparency around how I consent to the online learning platforms my children are using and how their data is being collected and used for other purposes. How do I know that these platforms are conforming to privacy regulations?

Recommendation: To develop national best practices and/or standardization solutions for accountability frameworks related to privacy and security of personal information.

Issue 2 — Certification for Professional Roles

Scope: The process of assessing the role of professionals working with data and information, assessing professional competencies requirements based on a clear framework representing the backbone of data governance.

User story: As a citizen, I want to know that the businesses I am trusting with my data are committed to upholding industry standards.

Recommendation: To develop criteria or standards for evaluating core competencies of data governance professionals.

Issue 3 — Digital Literacy

Scope: The process of improving the understanding of data, technology and interfaces for Canadian residents.

User story: As a citizen, I want to understand privacy settings and password protection, and to engage in online services in a safe environment.

Recommendation: To develop standards accessible to different parts of society such as youth, elders, vulnerable groups and communities for whom English or French are not their primary languages.

Issue 4 — Cybersecurity Protection

Scope: The process of creating cybersecurity protection and transparency, which are transversal components across the data governance framework; this includes digital, network and connectivity infrastructure, but does not cover directly IT security (physical aspect of the infrastructure).

User story: As a small company, how can I better manage cybersecurity protection and ensure my clients know they can trust my services?

Recommendation: To dedicate more efforts to cross-sectoral standardization solutions (and not sector-specific standards addressing resiliency and information security) for cybersecurity protection.

Issue 5 — Data Management Governance

Scope: The process of planning, creating oversight, monitoring and compliance of data management at the organizational level, aiming to clarify how data should be managed throughout its lifecycle.

User story: As a data management expert responsible for managing my organization's data management system, what tools or guidance are available to me to ensure my organization is optimizing its productivity, handling its security risks and making sound decisions?

Recommendation: To standardize organizational governance of data management adapted to different sizes and types of organizations.

Issue 6 — Data Privacy (consolidated with Issue: Data rights)

Scope: The process of determining who has the data rights, if the rights can be transferable, and who has the right to distribute data. Data control is becoming increasingly important, especially with Artificial Intelligence (AI) and Internet of Things (IoT) technology using and generating new data. Consequently, data generated by these new technologies should be equally transparent, compliant and fair, and have the data rights holders' consent. The Canadian Charter of Rights and Freedoms should also be used as a guiding document.

User story: As a citizen, what are my rights to my personal data? How are organizations that have my data complying with rules and legislation? How am I consenting to the use of my personal data?

Recommendation: To harmonize privacy and security legislation across Canada, specifically related to consent, using standardization solutions where appropriate.

Issue 7 — Guidance on Trustworthiness, Ethical and Societal Use of Data

Scope: The process of determining trustworthiness and ethical use of data in accordance with the Canadian privacy expectations specified in PIPEDA and the Privacy Act; clarifying the ethical use of data with respect to who owns data, including the ethical and societal use of data according to public values.

User story: As a citizen, how do I know if an organization is abiding with or conforming to PIPEDA or the Privacy Act? What assurances do I have?

Recommendation: To standardize the responsibilities of all actors involved in the data lifecycle.

Issue 8 — Harmonization and Interoperability of Data Practices/Open Data

Scope: The process of harmonization of data practices with the aim of characterizing how technology, processes and systems work together. This issue also explores the role of policy, legal and business practices to support seamless interaction between businesses and industries. Consequently, it must focus on a high-level interoperability (rather than looking at technical practices), particularly the ability for data to be exchanged between platforms with the highest fidelity and minimum intervention while ensuring privacy and security.

User story: Working in a health-care organization, I need rapid integration of data that comes from various sources. I require practices and policies to be harmonized to assess the interoperability needs of the health ecosystem that I work in, while also protecting patient privacy.

Recommendation: To promote harmonization and interoperability for new technologies and practices, supported by standardization solutions where applicable.

Issue 9 — Data Actor and Data Transaction Roles

Scope: The process of exploring the roles of data actors throughout the lifecycle of the supply chain and highlighting the responsibilities and accountabilities of data professionals. Between data collection and data consumption, there are many layers of data management processes. Numerous people and computer systems are involved through the lifecycle of even a single data element. Whether it is securing the data from unauthorized access or taking daily backups for example, these different actors are accountable for protecting data through the formation of a secure system that reduces any risk of errors. Standard terminology on the roles that each computer system (and users) plays, and what this means for the roles of data provider, data consumer, data broker, data user, data repository, etc.)

User story: As a citizen, how do I know if an organization is using qualified data professionals to manage my information (or the organization's)? What type of accountability do those professionals have?

Recommendation: To develop a foundation of cross-sectoral standards to help facilitate the oversight of data professionals from one sector to another.

Issue 10 — Secondary Use of Data

Scope: The process of using data for purposes other than those for which it was originally collected. Secondary use of data includes using data for a different purpose than what the data rights holder had initially consented to and for which explicit consent was not received. This issue explores the possibility to delete data and withdraw consent, and the expiration of data consent.

User Story: As a citizen, how do I know if my data is being sold to secondary users and how can I consent to this?

Recommendation: To develop best practices to facilitate dynamic consent management and enable the use of de-identified information, under strong governance frameworks and standardization, as a competitive advantage.

Working Group 2: Data Collection, Organization, and Grading

Issue 11 — Data Collection

Scope: The process of gathering and measuring information on variables of interest. Determining the importance of understanding whether the acquisition of data appropriately balances the need for data with the means used to collect it.

User story: As a citizen whose data is hosted on multiple data storage platforms, it is vital that I have the confidence in these platforms. A system or tool that can assess whether my data is collected in a fashion that ensures ethical data acquisition principles is critical.

Recommendation: To standardize this practice and to cover the three areas of data source categories (analog, digital, streaming).

Issue 12 — Data Systems Management

Scope: The process of managing information systems to ensure interoperability and security with respect to systems design, encryption and access controls.

User story: As a citizen, oversight is required to ensure that data systems are designed with access controls to integrate different types of data and transform it so that it can be safely consumed.

Recommendation: To standardize the ability for systems to communicate between mechanisms and devices. It is important to clarify whether the data systems management would depend on the type of data sitting in the system and whether there is a need for different sets of standards to address this matter. For example, data systems management could be classified as an application system that ingests, manipulates and deletes data. There is a need to determine if standards are being followed in accordance with the operations or steps of the data lifecycle.

Issue 13 — Discoverability of the Data

Scope: The process of knowing what data sets and sources exist, how to find them, and how to use them. This process does not include the notion that the ability to discover data guarantees access to the data.

User story: As a citizen whose data is hosted on various data platforms, I need to have the opportunity to search information stored about me with ease.

Recommendation: To standardize the way in which data retrieval systems are set up, including a taxonomy of existing data. The importance of knowing how data is interpreted, digitized, captured and formatted is key as it relates to how data is interpreted and analyzed for linkage purposes.

Issue 14 — Data Linkage

Scope: The process of combining information from two or more sources to create a richer dataset. Data linkage addresses the elements of consent and security as the data does not reside in the same place.

User story: As a citizen I need to have confidence in how my data will be used and linked. There needs to be better oversight of practices that have the ability to create personally identifiable information when linking two independent data files.

Recommendation: To standardize the practice of linking data while adhering to and addressing privacy implications. Data linkage creates an ethical dilemma and goes beyond the original purpose of the data collection process.

Issue 15 — Manual Tagging of Data

Scope: The process of manually augmenting data by adding specific codes instead of using an AI algorithm due to possible errors created by automated systems.

User story: As a citizen, I would be concerned about the way a system generates specific data. For example, if a facial recognition system carries a certain bias, there is a likelihood it leans towards generating specific results.

Recommendation: To standardize the practice of manually tagging data to create a diverse approach of reducing errors created by automated systems. The lack of a consensus approach gives rise to bias.

Issue 16 — Metadata Management

Scope: The process of managing data that provides information about other data. This practice entails an end-to-end process of collecting, managing, accessing and understanding the capabilities of the data. Metadata management, also known as data about data, can assess whether data is trustworthy.

User story: As a citizen, the ability to understand the terminologies that define data about data helps me identify whether stored data is trustworthy. For example, data results from clinical trials for a vaccine can provide further insights into the vaccine's efficacy.

Recommendation: To standardize the terminologies around the management of data about data.

Issue 17 — Organizational Data Policy Strategies and Risks Management

Scope: The process of ensuring compliance through the adoption of a data governance framework.

User story: As a citizen, I have more confidence in the data management systems when all the organizations' data policy and risk management frameworks follow a uniform approach to creating a data governance framework. For example, if telecom company A's data retention policy is to hold personal information for three years versus telecom company B's policy to hold personal information for seven years.

Recommendation: To standardize the approach of creating organizational data policy strategies and risk management frameworks.

Issue 18 — Data Quality and Fitness for Use Assessment

Scope: The process and all activities related to assessing the quality of data.

User story: As a citizen, I need to have confidence that data hosted by data stores is of high quality.

Recommendation: To standardize the frameworks put in place to understand, describe, measure, monitor, verify, attest and report on data quality.

Working Group 3: Data Access, Sharing, and Retention

Issue 19 — Consent Management (Consent, Access, and Withdrawal)

Scope: The process of managing the entire lifecycle of an explicit data use agreement (either a paper version or a digital version) between a data subject (or data owner) and a data controller (or data provider or data consumer).

User story: As a patient giving consent to a health-care provider to collect data about me for diagnostic purposes, I need to have the opportunity to withdraw my consent so that I prevent the further use of my data when my clinical case is closed.

Recommendation: To standardize such agreements and how they cover either a specific data item (fine grained) or a broad range of data topics (coarse grained) either acquired in the past or expected to be acquired in the future; how the digital forms of such agreements are managed throughout their lifecycle; whether and how they accompany each data transfer and exchange; and how their withdrawal may impact the data already shared.

Issue 20 — Data Access

Scope: The process of establishing a connection between a data provider and one or more data consumers with the purpose of data retrieval, which includes dataset selection, establishing and negotiating bilateral or multi-lateral data use contracts, as well as enforcing the policies and restrictions in these contracts.

User story: As a data provider giving access to a dataset, I need to be able to prevent the data consumer from passing the same dataset to a third party so that I retain full control over my data.

Recommendation: To standardize how data providers and data consumers establish and negotiate data access contracts with usage policies that are both machine and human readable, and therefore interoperable, and how these contracts with their restrictions and obligations are being enforced during data retrieval and further along when the data has been delivered to a data consumer.

Issue 21 — Data Retention

Scope: The process of managing the information about what happens to a data item throughout its entire lifecycle — how it is acquired, how it flows between data actors, how it is modified and what new data is being created from (or related to) it.

User story: As a data owner who uses a data provider to host my data, I need to be able to define the rules that govern the retention of my data so that I can be sure that I will never lose important information.

Recommendation: To standardize how to express retention rules and policies that will govern how data custodians manage the lifecycle of data, including archiving, transforming, compacting and decommissioning data in their repositories in a way that is secure, transparent, portable, and compliant. This should also include aspects of discontinued data formats and tools that, if not handled properly, might render retained data unusable.

Issue 22 — Identity Management — Validation and Authentication (People, Entities & Devices)

Scope: The process of management and use of digital credentials for the purpose of identifying that a data actor (a person, organization or device) is the entity it claims to be, which in turn allows it to enter digitally and securely into data use contracts and data transactions.

User story: As a citizen, I need to be able to select an identity provider of my choice so I can digitally sign consent documents.

Recommendation: To standardize the way digital credentials are issued, used and managed so the actors they identify (persons, organizations and devices) can securely participate in data transactions. This includes federation and authentication across identity networks both for the purposes of adherence to data access policies and restrictions when exchanging data and for identifying who participated in past transactions.

Issue 23 — Data Sharing, Exchange, and Integration

Scope: The governing principles around sharing, exchange and integration of data and how they can be expressed in standardized contracts. As data is a non-rivalry resource (can be copied and used simultaneously), data owners need mechanisms to exercise their data sovereignty after their data is shared or integrated in an asset over which they have no direct control.

User story: As a data owner, I need a way to define how my data can be shared, exchanged and integrated into other products and services so that I contribute to causes I care about.

Recommendation: To standardize the data sharing agreements and/or frameworks with a focus on their contractual rather than technical aspects, including all types of data sharing and exchange scenarios (bilateral, multilateral and decentralized) as well as data integration — when data is embedded and becomes an integral part of another asset (a product, a service or aggregation).

Issue 24 — Trusted Data Intermediaries

Scope: The role that data intermediaries (such as data brokers, data trusts, data unions and collectives) play in the data ecosystem by providing independent, fiduciary stewardship of data either temporarily or permanently and how this may enable storing and managing data separately from the applications that generate or use it.

User story: As a citizen, I need to be able to use an independent data union to which my financial services should send my data and from which I can enable other financial services to request this data so that I keep all my financial records in one place.

Recommendation: To develop standards that any data intermediary will need to adhere to for independently storing and/or brokering data between parties and be “trusted” by the ecosystem. Also, to clarify whether, or under what conditions, such data intermediaries can make decisions on data on behalf of the data owners and how they would comply with any data use contracts set by these owners who may temporarily or permanently transfer data under their custody.

Issue 25 — Authorization for Data Collection and Sharing

Scope: The policies that govern data collection of both personal and industrial/commercial data and the permissions, restrictions and obligations the actors who perform this collection have in further sharing the acquired data. This includes the mechanisms that enforce these policies and provide transparency on this enforcement while protecting any sensitive information.

User story: As a citizen, I want to have full transparency about who is authorized to collect data about me and for what purposes so I have the full guarantee that my privacy is being respected.

Recommendation: To standardize the policies around data collection and how this collection is authorized, how this authorization is enforced, under which circumstances the collected data can be processed and shared as aggregate information, and whether/when individual data is allowed to be extracted from such aggregate datasets.

Issue 26 — Encryption

Scope: The policies and standards that govern the use of the technical tools to codify confidential information in all stages of its lifecycle — while the data is at rest, when data is in transit, and when data is used. This includes the type of encryption (including homomorphic encryption), the strength of the encryption, its enforcement, its use to ensure data integrity, and which actors can further process encrypted data (including its decryption) and under which circumstances.

User story: As a data owner, I want to be sure that my data will be encrypted by all data actors in all data transactions and only decrypted by those with whom I share my private key(s) or to which I have given explicit consent.

Recommendation: To standardize the use of encryption and its acceptance criteria for conforming to privacy and confidentiality rules while using data which takes into account the advances that new technological development (such as quantum computing) may bring.

Issue 27 — Management of Ontologies

Scope: The management of individual ontologies (vocabularies of concepts, hierarchies and relationships), as well as the way to organize multiple ontologies by grouping, merging and mapping between them and how they can be used in coding practices.

User story: As a data consumer, I need to be able to translate the dataset that a data provider delivers to me into the ontology of my choice so that I can interpret the data in my own terminology.

Recommendation: To standardize the management of ontologies (vocabularies of concepts, hierarchies, relationships, etc.) and their lifecycle (from concept definition to discontinuation), as well as their application in describing data and its semantics, including complex coding practices such as post- and pre-coordination, and also the way data consumers can get access to the ontology that describes the dataset they retrieve.

Issue 28 — Data Transparency, Lineage, and Traceability

Scope: The process of managing the information about the handling and treatment of a data item throughout its entire lifecycle — how it is acquired, how it flows between data actors, how it is modified and what new data is being created from (or related to) it.

User story: As a citizen who uses the city public infrastructure, I need to know what mobility data has been collected about me, who has used this data and for what purposes so that I understand my contribution to building a smart city.

Recommendation: To standardize the information captured about a data item when it is acquired, exchanged, modified and used as a source for other data creation or analysis; who can access such meta information and under what circumstances; how should this meta information be protected, retained and disposed of independently of the data item it describes.

Issue 29 — Data Portability and Mobility

Scope: The right to data portability allows data subjects to receive personal data they provided to a data controller in a structured, commonly used and machine-readable format. Additionally, providing the ability to transmit that data in a secure manner to another controller.

User story: As a citizen who uses a social media network, I need to be able to request that all my data in that network is exported in a digital format so that I can then choose to store it in another repository of my choice.

Recommendation: To standardize the preservation of information exchange between systems so data can be exported in a digital format by data controllers with its detailed structure, its metadata and links to other data. Also, under which circumstances data about data subjects can be removed by a data controller and the implications this has on other related data (e.g., the right to be forgotten).

Working Group 4: Data Analytics, Solutions, and Commercialization

Issue 30 — Technical Elements of AI Solutions

Scope: The technical components and lifecycle of the AI solutions, referring to systems, technologies, software and platforms, and the development, analysis, verification and validation of them. This includes the terminology used, including artificial intelligence itself, the subcategories of artificial intelligence, describing the lifecycle and individual components.

User story: As a citizen or as an AI practitioner, I want an understanding of terminology that is used to describe solutions that use my data and have assurance that it works in the way that it says it does.

Recommendation: To standardize terminology and the lifecycle components to lay the groundwork for the interoperability of AI solutions, and specifications for verification and validation.

Issue 31 — Data Value Chain

Scope: The monetary value creation at different stages of a data supply chain. A process of identifying monetization and valuation of data, and its role in intellectual property.

User story: As a citizen, I want to be sure I am receiving a fair return on the data that I part with. As a data enterprise, I am interested in the monetization of data and its revenue potential for my business.

Recommendation: To standardize the system by which valuation is applied to data, and its implications for data exchanges and transactions.

Issue 32 — Transparency and Communication of Data Analytics

Scope: The process of disclosing and communicating data analytics, as well as disclosure of exposure to risks for data owners from the perspective of the data supply chain.

User story: As a data owner (citizen), I want to know what happens with my data and whether there are any risks associated with sharing.

Recommendation: To standardize the process and terminology by which data owners are informed of what happens to their data and what possible risks sharing their data may incur.

Issue 33 — Interpretability and Explainability of AI Systems (Originally “Interpretability of Algorithms.)

Scope: The process of explaining the results, capabilities and functions of an algorithm. Explainability in this context means that results of solutions can be explained in human terms.

User story: As a citizen, I can come into contact with AI solutions through the products and services I use. I want to know what the AI solution capabilities are, what sort of outcomes and/or decisions the AI solution can make and *why* it made that decision.

Recommendation: To standardize the way that AI system capabilities and results are explained in human terms.

Issue 34 — Assessment and Management of Bias

Scope: The process of identifying bias and, where necessary, managing bias.

User story: As a citizen, I want to ensure that I am not exposed to bias or discrimination against me due to a decision made by, or with assistance from, an AI solution, particularly when it may influence a decision about me, such as pertaining to my finances, insurance or health.

Recommendation: To standardize the types of protocols, processes and assessments used in identifying bias, as well as standardizing the management of bias where necessary.

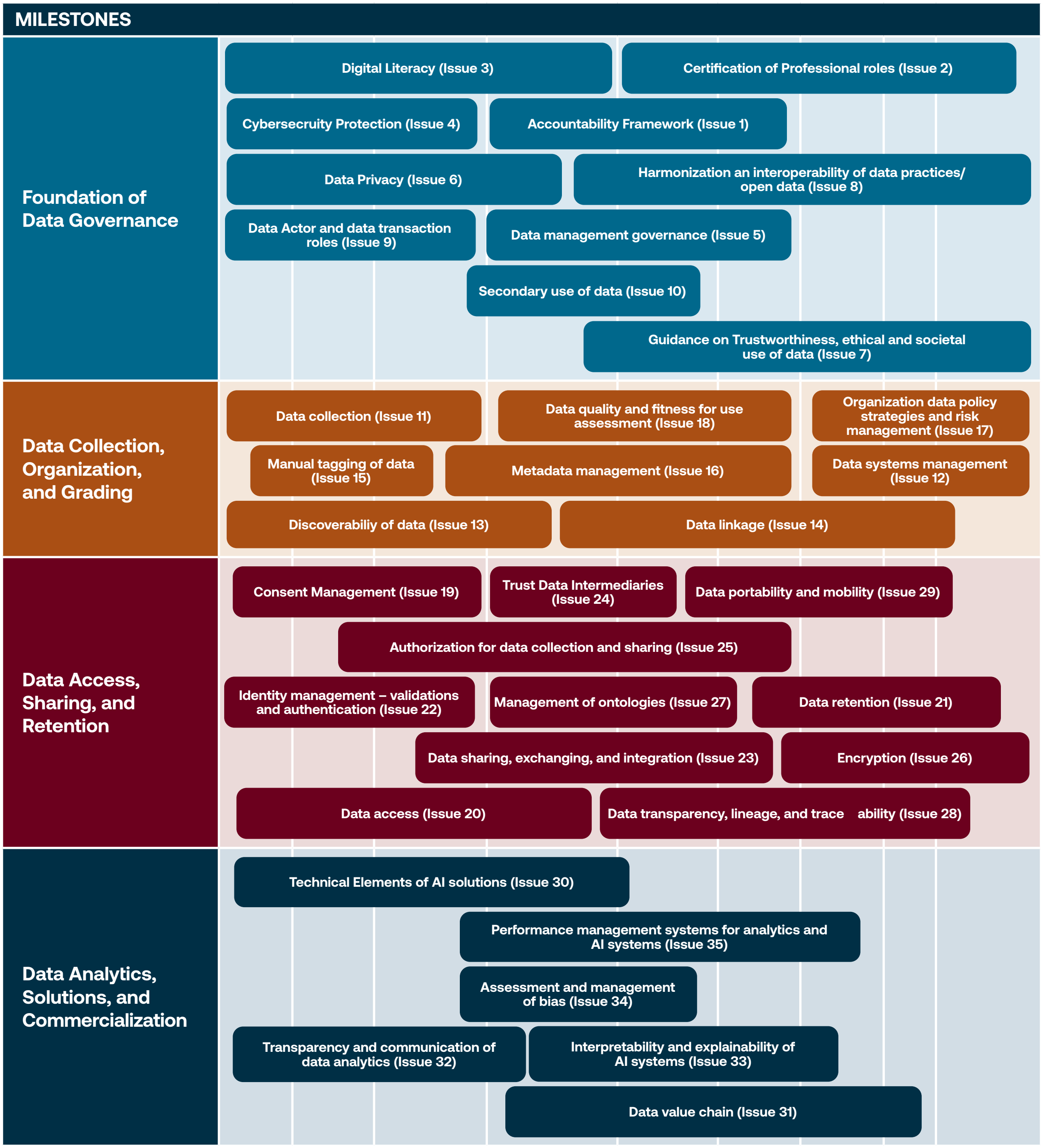
Issue 35 — Performance Management Systems for Analytics and AI Systems

Scope: The process of establishing internal governance, from the analysis of risk level to the design and deployment of models, algorithms and systems.

User story: As a citizen, I want assurance that organizations that develop or use AI solutions have the right processes in place to ensure the quality of the systems they create/use and the right processes in place to manage any adverse or unexpected events.

Recommendation: To standardize the governance approaches in organizations that use or create AI systems, encouraging diverse participation in the development of conformity assessment-based standards such as ISO/IEC 42001 Artificial Intelligence Management System Standard.

Diagram 3: Proposed Timeline for Implementation of the Roadmap



MILESTONES

Foundation of Data Governance

- Digital Literacy (Issue 3)
- Certification of Professional roles (Issue 2)
- Cybersecruity Protection (Issue 4)
- Accountability Framework (Issue 1)
- Data Privacy (Issue 6)
- Harmonization an interoperability of data practices/ open data (Issue 8)
- Data Actor and data transaction roles (Issue 9)
- Data management governance (Issue 5)
- Secondary use of data (Issue 10)
- Guidance on Trustworthiness, ethical and societal use of data (Issue 7)

Data Collection, Organization, and Grading

- Data collection (Issue 11)
- Data quality and fitness for use assessment (Issue 18)
- Organization data policy strategies and risk management (Issue 17)
- Manual tagging of data (Issue 15)
- Metadata management (Issue 16)
- Data systems management (Issue 12)
- Discoverabiliy of data (Issue 13)
- Data linkage (Issue 14)

Data Access, Sharing, and Retention

- Consent Management (Issue 19)
- Trust Data Intermediaries (Issue 24)
- Data portability and mobility (Issue 29)
- Authorization for data collection and sharing (Issue 25)
- Identity management – validations and authentication (Issue 22)
- Management of ontologies (Issue 27)
- Data retention (Issue 21)
- Data sharing, exchanging, and integration (Issue 23)
- Encryption (Issue 26)
- Data access (Issue 20)
- Data transparency, lineage, and trace ability (Issue 28)

Data Analytics, Solutions, and Commercialization

- Technical Elements of AI solutions (Issue 30)
- Performance management systems for analytics and AI systems (Issue 35)
- Assessment and management of bias (Issue 34)
- Transparency and communication of data analytics (Issue 32)
- Interpretability and explainability of AI systems (Issue 33)
- Data value chain (Issue 31)

Next Steps

This Roadmap is a first iteration to develop a common lexicon and language for all stakeholders that are struggling with how to evolve their data strategies and frameworks, driven by tech opportunities, policy and competitive pressure. It provides a pathway through standardization towards consistent understanding and implementation of strategic and operational data governance issues that Canada (and other countries) is now facing.

The agility of the standardization system in moving goalposts is a call to action to help us grapple with new notions, such as de-identification and anonymization brought forward by new privacy laws, such as Bill-64 and Bill C-11, or rules regarding the use and management of artificial intelligence systems in emerging global regulations. The line between where standardization can really provide value and support as a tool and where we need policy or other factors to help move the vision forward will be key. The standardization mapping is valuable immediately, but given that technology is moving quickly, the standardization landscape is out of date as soon as its published. Canada and related ecosystems will benefit from the continuance of this Collaborative to provide an opportunity to revisit this work at intervals, to keep the Roadmap up to date, and to oversee the implementation of its recommendations as a pan-Canadian effort.

According to Diagram 3, there are dozens of issues we need to work on right now, starting with Digital Literacy, Cybersecurity and Privacy. Implementation of the 35 recommendations will require support and leadership for the adoption, adaption or development of standards and conformity assessment activities that help to close current gaps. It will also require detailed analysis and action plans for each of the 35 key issues and the outcomes of the use case working groups, Indigenous engagement and the standardization landscape so that activities already under development take into account current standards, best practices or other normative type documents as initiatives evolve.

Likewise, Indigenous engagement recommendations need to be directly part of this implementation plan, including: (1) outreach in a more fulsome way to Métis and Inuit organizations, rights holders and stakeholders who are not well represented in this first Roadmap; (2) involving Indigenous groups to tie the findings of the Firelight Group engagement directly to those issues developed by the use case working groups, where appropriate; and (3) including Indigenous organizations and the First Nations Information Governance Centre in further phases of the work, including standards development. From an implementation point of view, ensuring resources are available to Indigenous organizations to enable participation in a meaningful way needs to be considered.

Standardization in Action

Implementation of and ongoing updates to this Roadmap will require continued commitment from a Steering Committee and Collaborative members, in addition to ongoing funding to continue to guide, coordinate and enhance standardization activities to enable the market for a digital economy to thrive.

Short-term outcomes of this will include continued oversight of the Collaborative and its governance, and communication and promotion of the Roadmap to stakeholders. An action plan for the 35 recommendations will be developed within the first two years with the support of the Collaborative.

With the support of Statistics Canada, a dashboard will be created to track the implementation of the recommendations and the status of closing the identified gaps.

Action plans for the 35 recommendations will position Canada to:

- Become a standards setter and influencer internationally in the sphere of data governance/big data;
- Lead the development of new national and international standards and conformity assessment schemes;
- Increase its participation and influence in relevant standards-development committees;
- Enter into international standardization agreements that support Canadian public policies and government priorities;
- Advance harmonization and alignment internally among different jurisdictions;
- Advocate for standardization as a tool to achieve regulatory and economic objectives;
- Advance standardization solutions that are responsive to evolving and emerging sectors;
- Promote and protect the IP of innovative Canadian businesses through standardization;
- Leverage its innovation and IP into standardization solutions; and,
- Protect the health and safety of Canadians through standardization solutions that are based on quality, trust and ethics.

This is expected to lead to the development of new international standards and conformity assessment schemes which will help ensure that the interests and priorities of Canadian businesses are promoted and protected, thus providing Canadians with greater security, privacy and control of their data and enabling safe and secure commercialization of data.

A second version of the Roadmap will commence in 2021 to address new issues that were not covered in this first version, and to provide an update on the work related to the implementation of recommendations.

Annex A —

Gap Analysis of Standards and Specifications

This roadmap section sets forth a description of key issues, relevant published standards and specifications, and those in development; recommendations on the need for additional R&D and/or standards and specifications, as well as priorities for their development; and the organization(s) that potentially could perform the work. It is divided into several sections corresponding to the DGSC working groups: Foundations of Data Governance; Data Collection, Organization and Grading; Data Access, Sharing and Retention; and Data Analytics, Solutions and Commercialization. It is noted that recommendations on organization(s) that could potentially perform work should not be viewed as conclusive or in any order of preference or authority.

Working Group 1: Foundations of Data Governance

Issue 1 — Accountability Framework

This issue covers the liability and the control structure for all data collected and created, and clarifies the roles, responsibility and accountability of data transaction. The responsibility of the data rights holder, the implication of ownership transfers, and the notion of consent was also explored. Accordingly, the aim is to develop an accountability model for an organization in the context of its data supply chain(s). The accountability framework should provide the necessary tools to organizations to ensure compliance and accountability vis-à-vis data regulations. There is a wide range of consent regimes that should be assessed to enhance transparency, rather than limiting the definition to the main consent forms favoured by large organizations. The lack of consistent definition around consent needs to be addressed in standards to help guide data governance. The accountability framework should also explore the role of identity management and the traceability of data throughout its lifecycle.

The lack of standards for identity management and consent have made it difficult to develop a rigorous accountability framework and impede the development of regulations. Traceability and accountability tools need to be developed as data users are often not given fair notice on how their data will be used in both the short-term and long-term use of data. There is a strong need to better harmonize the development of standards in accordance with regulations to facilitate compliance and implementation. There is a need to be clear in how consent is applied. The difference between implicit and explicit consent for the purpose of use should also be clarified.

Laws across Canadian jurisdictions differ and may represent an issue for the implementation of an accountability framework unless there is harmonization. There is a need to determine how the different lines of responsibility interact with each other. For instance, clarifications are needed for when provinces declare a state of emergency to better understand the impact across Canada. The most recent example of this situation happened during the health crisis related to COVID-19 where provinces declared a state of emergency which impacted data controls and regulation. This event will provide us with the opportunity to review the current system and improve the data sharing mechanisms in Canada. Accordingly, best practices and guidelines should be developed to improve data management in times of crisis for the public good.

Gap: Accountability Framework. The standard search generated a large number of standards related to this issue; however, very few were categorized as relevant. Most standards found are specific to a sector, mainly health and transportation, and a majority of standards only partially matched the issue. Interestingly, more than half of the standards deemed relevant were published in 2017 or after, which indicates a strong effort to provide the right standardization tools for better accountability in data governance. There is no definitive gap that was identified from the standard search. The uptake in standardization activities regarding accountability will provide a variety of tools for organizations to enhance their responsibilities over their data management. The main challenge for organizations will be to navigate the different data privacy regulations emerging across different jurisdictions and align the standards with these various regulations.

Is R&D Needed? Yes

Recommendation: To develop national best practices for accountability frameworks related to privacy and security of personal information.

Priority: Medium

Organization(s): Office of Chief Information and Privacy Commission in jurisdictions and at federal level

Issue 2 —
Certification for Professional Roles

This issue clarifies the role of professionals working with data and information, explores certifications programs that should be developed, and the requirement of the industry. This issue should first be addressed by assessing professional competencies requirements based on a clear framework representing the backbone of data governance. This framework should reflect the sector's needs and the fast pace of innovation, and encourage innovation rather than prevent it. Due to the sensitivity of their role, professionals working with data have an obligation to society. Accordingly, the role of Professional Associations, with mandatory professional standards overriding employers' requirements, should be considered to prevent wrongdoing. There is a need to protect the people and organizations.

It is difficult to develop a certification program for an innovative sector with very few standards and regulations in place. Certification programs for such a large and nascent sector may be difficult to implement across multiple industries. There may be need for industry-specific certification in addition to broad certification for data as a discipline (e.g., there is already certification for health data for coding — see CHIMA). Additionally, there is a risk of codifying a profession that will constantly grow and change. That is why a framework should be identified before the development of certification programs. The implementation of standards and certification programs should be reflected in regulation and monitored to prevent the creation of a false sense of security. Similarly, best practices and guidelines should be shared within organizations to raise awareness among managers and other employees.

Awareness and education on the use of and risk around data should be offered in schools to protect children and young adults since they are especially vulnerable to data breaches. In fact, while professional training is important, there is also a need for educational programs in universities and colleges to provide a broad understanding to the future generation of workers. This awareness at a young age will ensure better practices within organizations and will better protect our societies.

Gap: Certification for Professional Roles. The standard search related to Certification for Professional Roles generated a limited number of qualification and certification schemes for organizations and professionals from a standards perspective. Most standards were categorized as non-relevant to the issue and very few were deemed relevant. The standard search reflects the difficulty in developing standards for professional roles in such a high-pace sector, as highlighted in this issue description. The search also provided sector-specific standards and standards indirectly related to the issue that could be relevant for the development of cross-sectoral standardization solutions for data professionals. Therefore, the standard search underlines a clear standardization gap related to this issue and confirms that efforts must be dedicated to provide better support to data professionals through standardization.

Is R&D Needed? Yes

Recommendation: To develop criteria for evaluating core competencies of data governance professionals.

Priority: Medium/Low.

Organization(s): DAMA (Data Management Association), CHIMA (Canadian Health Information Management Association), Digital Health Canada, EDMC (Enterprise Data Management Council), HIMSS (Healthcare Information and Management Systems Society), IAPP (International Association of Privacy Professionals)

Issue 3 — Digital Literacy

It was determined this issue will cover digital literacy by focusing on improving the understanding of data, technology and interfaces of Canadian residents. Digital literacy must be kept separate from professional certification and have a broader mandate, including the use of technologies effectively and securely. Education represents a key mechanism to raise Canadians' awareness about the challenges and opportunities of an increasingly digital society, which is necessary for the implementation of an efficient and inclusive data governance framework. Ultimately, data governance is about sharing responsibilities between multiple actors, including consumers. For instance, Canadians should have the appropriate tools and knowledge to identify fake information circulating on the web and understand the use of their data in analytics. The issue will also discuss how the education should be provided, who should be responsible for providing the education, and what the Government's role will be in ensuring harmonization across provinces.

Education should be better coordinated between private organizations and Governments to avoid duplicating efforts and ensure synchronization. Accordingly, clear objectives need to be determined to avoid confusion and provide a useful and reliable education. Significant efforts will have to be dedicated to educating and protecting vulnerable populations and promoting an inclusive approach to digital literacy. The fast rate of innovation and change will represent a major challenge to maintain a reasonable level of digital literacy in the population. Thus, the education curriculum will have to be constantly updated and continuously offered to the Canadian population.

Digital literacy frameworks have already started to emerge in Canada providing key education on technology to children. For instance, the Yukon Territory released the Yukon Education Digital Literacy Framework, which offer guidelines to help teachers provide core technological competencies to students. This type of initiative should certainly be replicated across Canada and adapted to different age categories. Digital literacy guidelines should not be limited to educational institutions and could be offered through media or community centres to reach all the populations. The goal is to democratize the use and understanding of technology. Moreover, there should be more collaboration between Governments and industry to offer different types of education programs covering various sectors. For instance, private organizations in the health sector have already collaborated with academia and the Government to enhance the use of technology and data in the health sector, and this should be replicated in other sectors. Similar initiatives can also be seen in Finland and Europe with the educational platform Elements of AI.

Gap: Digital Literacy. The standard search for the Digital Literacy issue generated very few standards, including indirectly relevant standards and sector-specific standards. The results of the standards landscape reflect the recent emergence of this issue and the growing importance of civil society in data and technology. In fact, standards that address digital literacy are mainly developed for youth and formal educational institutions, overlooking a large part of the population. The limited information available for civil society is very granular and not adapted to the needs and aptitudes of the active population and the elders. This gap highlights an urgent need for standardization to protect vulnerable groups from the risk related to data privacy. This important gap will definitely need a more important participation rate by civil society in standardization activities to ensure that their specific needs are addressed.

Is R&D Needed? Yes

Recommendation: To develop standards accessible to different parts of society such as youth, elders, vulnerable groups and communities for whom English or French are not their primary languages.

Priority: High.

Organization(s): P/T Ministries of Education, Universities and Colleges, Media Outlets, Teachers' Associations, College of Teachers (regulatory body)

Issue 4 —
Cybersecurity Protection

This issue covers cybersecurity protection and transparency, which are transversal components across the data governance framework. Cybersecurity threats will increase with the rise of technology and will require stronger mechanisms to protect data and sensitive information. The core of cybersecurity risks is related to digital, network and connectivity infrastructure. Thus, although there is a strong relationship, the issue will not directly cover IT security, which covers the physical aspect of the infrastructure. A differentiation between infrastructure security, personnel security and individual responsibility toward cybersecurity should be performed to clarify the role of each actor.[16]

The first obstacle that must be addressed is the lack of consistency for the cybersecurity protection definition. The multitude of standards addressing cybersecurity prevent national and international harmonization and the adoption of consistent regulation across countries and regions. Accordingly, this creates unequal cybersecurity systems among organizations, leaving more vulnerable people at a higher risk. The increase of cybersecurity should also be accompanied by an increase in transparency rather than secrecy. To trust the efficiency of cybersecurity, it must be transparent. Therefore, a sound balance between transparency and secrecy will enhance the cybersecurity protection, whereas a rise in secrecy could be dangerous.

Cybersecurity protection should be embedded in all the new technologies that are being developed. In fact, it is much easier to embed cybersecurity technology during the development process than adding cybersecurity protection to an old technology. Cybersecurity should also be treated as a national priority for the Government. For instance, a cybersecurity provision was included in the Canada-United-States-Mexico Agreement (CUSMA) recognizing that cybersecurity threats can undermine digital trade. CUSMA also encourages member countries to use a risk-based approach to cybersecurity rather than a prescriptive one and to rely on consensus-based standards (Article 19.15 (2)). In this respect, Canada developed a CyberSecure Certification Program to help Canadian organizations better manage their cybersecurity protection. However, there is still a lot of work to be done to harmonize standards and regulations across jurisdictions.

[16] For further clarification, see Schedule 1, Clause 4 .7 of PIPEDA clause 4.7 https://laws-lois.justice.gc.ca/eng/acts/P-8.6/page-11.html#h-417659 Clause 4 .7 requires organizations to apply "physical, technological and administrative" measures to protect personal information. Cybersecurity therefore includes, for example, secure areas for servers, firewalls and anti-virus for systems and strict administrative management of access privileges to information on the basis of need-to-know. It cannot be more specific than that because it will change as cybersecurity risks change. The test is "whatever measure that was applied, was it appropriate to the level of sensitivity of the information?"

Gap: Cybersecurity Protection. The Cybersecurity Protection issue generated a very high number of standards. A large proportion of these standards are sector-specific, targeting among other things information technology (IT), transportation and infrastructure. A significant share of these sector-specific standards were addressing resiliency and information security. A large majority of the standards categorized as relevant were developed after 2010, suggesting an increase in standardization activities related to this issue in the last decade. Moreover, it is interesting to note that most of these standards are related to the risk management aspect of cybersecurity. The standards landscape highlights the great number of standardization activities related to cybersecurity, which is a positive sign, but it will be important to dedicate more efforts to cross-sectoral standardization solutions as they only represent a small share.

Is R&D Needed? Yes

Recommendation: To dedicate more efforts to cross-sectoral standardization solutions (and not sector-specific standards addressing resiliency and information security) for cybersecurity protection.

Priority: High.

Organization(s): SCC-Accredited SDO

Issue 5 —
Data Management Governance

This issue explores the necessity of planning, oversight, monitoring and compliance of data management at the organizational level, aiming to clarify how data should be managed throughout its lifecycle. Data management should include the development, execution and supervision of plans, policies, programs and practices that control, protect, deliver and enhance the value of data and information assets. This issue should also consider a framework that will allow for the review of data management at the organizational level. A data management system will facilitate compliance with existing and future regulations. Accordingly, the data management system should be primarily developed with respect to PIPEDA and then could include variances for the different regulations across the world.

The scope and definition of data management differs greatly between regions and standards. However, without consensus on the function of data management, it is difficult for organizations to comply with regulations. Thus, clearer regulations should be developed to encourage organizations to manage data as assets and be legally accountable. Accordingly, we should examine existing best practices such as guidelines, assessments, tools and processes to transform into a comprehensive general framework. The general framework would be used by organizations and adapted to their respective objectives and sector. The data management framework should place an emphasis on performance objectives rather than being too prescriptive; this will provide more flexibility to organizations and will be easier to implement.

Each organization's goals and objectives should be linked to its data management policy, which needs to be understood by the steward (e.g., DAMA International covers the Data Steward type of role). Different data management models already exist and are used by large organizations, such as the Data Management Capability Assessment Model (DCAM) from the Enterprise Data Management Council (EDMC) which includes industry best practice and assesses capability from initial strategy through to execution. This framework is used by more than 60% of financial firms (100% of "Big Five" in Canada). The Canadian Institute for Health Information (CIHI) also offers a capability framework that identifies a few data management areas under policies and process.

Gap: Data Management Governance. There are few standards addressing Data Management Governance from an organizational and cross-sectoral perspective. Most standards that are directly or indirectly related to data governance are developed for specific sectors or pertain to physical systems rather than assisting in the lifecycle management of data. Furthermore, the majority of the sector-specific standards focus on a specific aspect of the data governance cycle, which makes it difficult for organizations to develop a complete data governance framework. Therefore, due to the lack of comprehensive standards covering internal practices, policies and supervisions, there is a gap to be filled in cross-sectoral and organizational data management governance. However, the large collection of sector-specific standards could be used as foundations for the development of organizational standards. Indeed, several standards in transportation, health and energy can be expanded to cover other sectors.

Is R&D Needed? Yes

Recommendation: To standardize organizational governance of data management adapted to different sizes and types of organizations.

Priority: Medium.

Organization(s): DAMA International

Issue 6 —
Data Privacy (consolidated with Issue: Data Rights)

This issue covers personal information and control of personal information. The definition and application of data privacy and data rights differ greatly from one regulation to another. It is important to determine who has the data rights, if the rights can be transferable, and who has the right to distribute data. Data control is becoming increasingly important, especially with Artificial Intelligence (AI) and Internet of Things (IoT) technology using and generating new data. Consequently, data generated by these new technologies should be equally transparent, compliant and fair and have the data rights holder's consent. Data privacy should be reviewed against existing data regulations, and there should be an attempt to harmonize regulations and standards to facilitate implementation. For instance, Canada's digital charter should be compared and reviewed according to international standards and regulations. The Canadian Charter of Rights and Freedoms should also be used as a guiding document, as it would fall under data rights.

The concepts of data rights holder and control should be better defined when it relates to data privacy and transparency. For instance, the transfer of data rights, if completed through a consensual agreement, should be more regulated and more transparent to protect the initial data rights holder. The concept of data rights does not apply to data the same way it applies to regular property. This is especially true when more than one party is involved in the data; how should the rights be split in these situations? Even when data is owned, it does not indicate the right that owners have over it. In fact, there might be times when data rights need to be given up for emergency situations, but the rights of the data are still maintained.

Should the context impact the application of data rights and control for the greater good? The circumstances under which the Government accesses citizens' data and overrides the concept of data rights may need to be revisited. Similarly, should the data rights holder have the option to refuse such access? Times of crisis may require unique efforts from the Government; however, there should be clear criteria to determine what happens to the data after the crisis. Similarly, if data needs to be shared with a private organization (e.g., pharma company in times of health crisis), there should be mechanisms in place to ensure all data are deleted from the organization's database once the crisis has passed. Accordingly, distinguishing the different roles in data governance and their respective scope of rights should help to eliminate confusing context situations.

Gap: Data Privacy. This issue generated a large number of standards, especially around data transfer in the telecommunication and information technology (IT) industry. A large proportion of standards have been deemed relevant to the issue. The high number of relevant standards confirms the growing importance of data privacy in standardization activities during the last decade. Furthermore, the standard search also highlights the progress made in the health sector with regard to data privacy and confidentiality, with a high number of standards addressing these concerns. However, there seems to be a lack of standards addressing data rights and data stewardship, two major concerns highlighted in the issue description. Lastly, although there is some standardization work in progress related to emerging technologies such as AI, blockchain and big data, there seems to be a lack of standards related to these technologies.

Is R&D Needed? Yes

Recommendation: To harmonize privacy and security legislation across Canada, specifically related to consent.

Priority: High.

Organization(s): Office of Chief Information and Privacy Commission in jurisdictions and at federal level

Issue 7 —
Guidance on Trustworthiness, Ethical and Societal Use of Data

The issue explores trustworthiness and ethical use of data in accordance with the Canadian privacy expectations specified in PIPEDA and the Privacy Act. This issue aims to clarify the ethical use of data with respect to who owns or stewards data, and the ethical and societal use of data according to public value. There should be a better understanding of what it takes from data owners, data stewards, the public and providers to be trustworthy to collect, manage, hold and use data and to actively demonstrate this trustworthiness throughout the lifecycle. The scope of ethics also includes the extreme circumstances under which specific data protection should be lifted or adjusted (e.g., in the health sector with COVID-19, what are the challenges for ethical collection, sharing and use of data?). Similarly, this issue will explore the necessity to develop sector-specific ethical data practices.

Ensuring trustworthiness, ethical and societal use of data throughout the data lifecycle represents major challenges. There are many questions that must be clarified to ensure safer data usage (e.g., what data should be collected? Who should be allowed access to data? What insights should be targeted during the data analysis? What are the ethics of applying insights?). The high number of actors involved as well as the hand-off of data from one application to another makes it difficult to monitor the use of data. Without transparency and check-and-balance mechanisms to prevent wrongdoing, there will always be a risk. For instance, tracking the movement of people through their phones for health purposes (e.g., COVID-19) may create a risk of using the data with the wrong intention. In fact, digital modes of contact tracing present a range of ethical challenges to privacy, accountability, consent, autonomy, fairness and accessibility, among others. Decentralizing the data control and access may be part of the solution to improve trustworthiness (this model is already applied in the health sector).

There are already multiple frameworks that exist related to trustworthiness and ethical use of data. For instance, the Institute of Electrical and Electronics Engineers (IEEE) and ISO/IEC JTC 1/ SC42 have published standards covering these issues. There may be a need to harmonize the different definitions and frameworks offered by different organizations. Additionally, there are regulations in place such as the Privacy Act and PIPEDA that address these issues on a regulatory basis. However, it has been determined that there is a need for supplementary legislation and other instruments to ensure meaningful consent and transparency. This issue is important to ensure good usage of data by the industry and the Government. There have been examples around the world of political entities using data without their citizens' consent and unethically. Thus, there are strong political risks that must be considered in this issue.

Gap: Guidance on Trustworthiness, Ethical and Societal Use of Data. The scope of this issue generated a large number of standards, most of them indirectly relevant or sector specific. The sector-specific standards mainly address environment and transportation concerns over the use of data. Moreover, most standards related to this issue are very granular and do not appear to go over the responsibilities of all actors involved in the data lifecycle in detail. As mentioned in the issue description, one of the principal concerns around this issue is to maintain trustworthiness from one actor to another and ensure ethical use throughout the data lifecycle. In fact, more than half of the standards generated from the search are associated with data collection, leaving few standards addressing the other components of the data lifecycle. However, it is interesting to note that more than one-third of the standards examined for this issue were developed in 2015 or after, which indicates strong standardization activities aiming to address this issue.

Is R&D Needed? Yes

Recommendation: To standardize the responsibilities of all actors involved in the data lifecycle.

Priority: Medium/Low.

Organization(s): SCC-Accredited SDO, International SDO

Issue 8 —
Harmonization and Interoperability of Data Practices/Open Data

This issue covers harmonization of data practices and aims to characterize how technology, processes and systems work together. This issue also explores the role of policy, legal and business practices to support seamless interaction between businesses and industries. Consequently, it must focus on high-level interoperability rather than looking at technical practices; more particularly, the ability for data to be exchanged between platforms with highest fidelity and minimum intervention while ensuring privacy and security. There will be a need to define interoperability in terms of industry, context and governance. Similarly, the needs for more rigid schemes versus flexible schemes should be considered for strategic and operationalization purposes. The open data infrastructure, which provides the ability for third parties to use data that is made available, will also be explored here.

There is a strong need to define and promote interoperable practices. Interoperability does not imply providing data access to external actors but rather facilitating exchange of information when necessary. There are multiple layers that must be addressed to promote interoperable practices, starting by standardizing Terms & Services to a simple date format field, which can cause significant complications. Although there are already several existing standards promoting interoperability and harmonization of data practices, there is still a lack of use of these standards. Accordingly, standards should be better reflected in regulations to promote their use and facilitate business practices across businesses and jurisdictions. However, the political aspect of harmonization policy may impede such an initiative.

Interoperability focuses on different aspects within separate industries. For example, in the health sector there is a rapid integration of data that comes from various sources to provide good healthcare, which requires practices and policies to be harmonized to assess the interoperability needs of the health ecosystem. This sector has also developed clear boundaries and criteria to determine which data should and should not be interoperable to protect the patient’s privacy. In other sectors such as the financial industry there has been a convergence during the last few years toward the use of ISO standards (e.g., ISO 8583 and ISO 20022). Ultimately, industry should use more standards to provide individuals data that are already interoperable to their customers.

Gap: Harmonization and Interoperability of Data Practices/Open Data. A large proportion of standards generated from the search exercise were categorized as relevant to this issue or partially relevant. This significant number of relevant standards indicates strong standardization activities aiming to improve harmonization and data practices in data governance during the last few years. In fact, more than 90% of the relevant standards were published in the last five years. Moreover, the standards relevant to this issue were almost exclusively developed at the international level from standards development organizations such as ISO, IEC and ITU-T, which eases the possibilities of harmonization across jurisdictions. Interestingly, a limited number of standards are sector specific; this could suggest a desire from data practitioners to increase harmonization across different sectors. Therefore, there seems to be no large standardization gap for harmonization and data practice in data governance, but a high level of standardization activities. However, as new practices are being developed, it will be important to rapidly include these in the standardization conversation.

Is R&D Needed? No

Recommendation: Promoting harmonization and interoperability for new technologies and practices.

Priority: Medium/Low.

Organization(s): SCC-Accredited SDO, International SDO

Issue 9 —
Data Actor and Data Transaction Roles

This issue covers the roles of data actors throughout the lifecycle of the supply chain. Between the data collection and data consumption, there is a huge layer of data management processes. There are numerous people involved through the lifecycle of even a single data element, whether it is securing the data from unauthorized access or taking daily backups, for example. These different actors are then accountable for protecting data through the formation of a secure system that reduces any risks of errors. Thus, this issue highlights the responsibility of data professionals and the accountability of their role. The different models of accountability should also be analyzed in order to determine which model is the most efficient (e.g., personal accountability versus professional accountability).

The lack and inconsistency of rules for governance related to data control and liability represents a significant issue in ensuring accountable use of data by data professionals. The creation of data professional associations that would ensure compliance of all their members by retracting their designations if there is recurrent non-compliance by the members could represent a great tool to mitigate the absence of clear regulations. Additionally, data transactions are becoming more complex and require more and more actors throughout the lifecycle, which may represent challenges for compliance with laws or contracts that may not apply or change in different jurisdictions. Accordingly, there is an increasing need to map the lifecycle of data transactions and the actors involved. The use of algorithms also necessitates the development of accountability safeguards, standards and certification programs to ensure the compliance of the algorithms.

The rise of technology and data collection created a multitude of data roles in various industries that has to be defined and overseen by an overarching body. There are lists of data roles that have already been developed for specific sectors such as the finance industry by the Enterprise Data Management Council (EDMC). There are also broader frameworks, such as the Pan-Canadian Trust Framework, that promote the safe use of data and facilitate secure transactions that should be used across sectors. These frameworks should be promoted in the different regulations as a means to increase compliance. Regarding automated decision-making and the use of algorithms, the Government of Canada released the Directive on Automated Decision-Making and has developed an Algorithmic Impact Assessment tool which can help to assess and mitigate the impacts associated with deploying an automated decision system.

Gap: Data Actor and Data Transaction Roles. The standard search for the Data Actor and Data Transaction Roles issue generated a large proportion of non-relevant standards and sector-specific standards, focusing on sectors such as transportation and telecommunications. Interestingly, most sector-specific standards addressed the data roles, data supply chain and data transactions aspect of the issue, whereas the standards deemed relevant seem to focus more on accountability. This distinction is interesting and demonstrates the importance of sector-specific standards to address specific needs of data practitioners. There would certainly be a need to use these sector-specific standards, of which more than 85% were developed after 2010, as a foundation for the development of cross-sectoral standards (that are currently very limited) to facilitate the oversight of data professionals from one sector to another.

Is R&D Needed? Yes

Recommendation: To develop a foundation of cross-sectoral standards to help facilitate the oversight of data professionals from one sector to another.

Priority: High.

Organization(s): ISO/IEC, SCC-Accredited SDO

Issue 10 — Secondary Use of Data

This issue covers the secondary use of data, which is defined as the use of data that is not that for the use it was originally collected. Secondary use includes data used for a purpose that is different than what the data rights holder had initially consented to and for which explicit consent was not received. The consent notice should clearly explain the way the data will be used and the limitation of its usage to prevent disagreement between the data rights holder and the data user, as required by law. This issue will also explore the possibility to delete data and withdraw consent. It is also necessary to determine the expiration of data consent. For example, does data consent expire after the death of a patient in the hospital or after accounts are closed at a bank? It is also important to consider whether guidance on data anonymization is relevant and to what extent anonymization could play a role.

Secondary use of data is problematic if the data owner does not explicitly consent to the usage intended by the data user. This means each stage of the data usage should be explicitly described in the consent forms rather than implied. This could also prevent the unauthorized monetization of data. It has also been noted that to divide secondary use into read access versus write access may help reduce wrongful usage. For example, data stewards have read and write access as they might be correcting data, while data analysts and data scientists should only have reading access to analyze the data.

Secondary use of data can also be necessary to improve the functioning of some sectors and has significant benefits for consumers. For instance, secondary use of data in the financial world is necessary to transfer consumer track records to credit bureaus or other financial institutions. Similarly, within healthcare, anonymous data and the use of aggregated data are helpful in developing new policies and improving existing process. Therefore, if data are used for other purposes than initially agreed, it is important to properly inform the data rights holder and receive explicit consent in an open, secure and transparent means.

Gap: Secondary Use of Data. The standard search for this issue generated a small number of relevant standards. Most of the relevant standards appear to address the issue from a data access perspective while very few relevant standards seem to focus on consent, which was identified as the principal concern for this issue. Moreover, approximately half of the standards related to this issue are specific to a sector such as health, transportation and energy. Similarly, a large percentage of the sector-specific standards focus on data traceability and few on consent. Accordingly, there seems to be a general need to develop standards with consent for secondary use of data as their main focus, which could be used across different sectors. However, it is important to note that a major percentage of the standards related to this issue were developed in the last few years, which indicates that several standardization activities might be taking place to fill this gap.

Is R&D Needed? Yes

Recommendation: To develop best practices to facilitate dynamic consent management and enable the use of de-identified information, under strong governance frameworks, as a competitive advantage.

Priority: Medium.

Organization(s): CIHI (Canadian Institute for Health Information)

Working Group 2: Data Collection, Organization and Grading

Issue 11 — Data Collection

This issue covers primary collection and addresses when organizations, either public or from the private sector, collect data for their own purposes. The process prior to data collection and the process of data collection were explored. With respect to data collection, the need for an assessment of balance between the need for data and the means taken to acquire it was apparent. The ability to identify needs and research for existing similar data was also identified within the scope of the process prior to data collection. With respect to the process of data collection, adding, manipulating other data, data cleansing and potential aggregations need to consider the aggregation of data and other issues such as collection frequency and tools (such as forms, MPIs, web scraping, phones, etc.).

There is a need to identify the existence of standards for the collection of various sources of data, be it geospatial, censors, survey or web sources, and their applicability to other types of data as a means to assess and identify gaps. Data sources can be categorized under three areas: (1) analog data, referring to data as it was received and managed in the past; (2) digital, referring to any source that is static but can be obtained, stored, manipulated and processed digitally; and (3) streaming, dynamic data, referring to IoT devices, sensors, etc.

The recording of attributes of the data collected — metadata — to assess quality was also explored. As illustrated by the COVID-19 pandemic, the representativeness and inclusivity of data, specifically when it pertains to populations, is of immense importance. Accordingly, the inclusion of these "principles" of data collection in the framing of this issue is necessary. In addition, there is also a need to ensure that data collected can be disaggregated, by sex, age and province/territory to enable users to account for disparities within a population when analyzing their data. An assessment of the credibility of the data provider and collector is also important in the framing of this issue.

Gap: Data Collection. The standard search generated a large number of standards related to this issue, with 20% of them identified as Tier 1 or Tier 2 standards. Most of the standards deemed the most relevant are related to data collection from Internet of Things (IoT) devices from the ITU-T series Y. ISO 8000 generic standard on data quality provides some guidance on data collection as well as ISO 14048, which covers Lifecycle Assessment – Data Documentation Form. Satellite data collection seems covered as well. Regarding the other items identified as part of the scope of this issue, it seems many standards exist but the vast majority of them are very specific to a data type or to data for a specific purpose. These specific standards could represent the foundation of a more generic standard but at the moment it seems there is a gap for the process pre-collection, the process of collection itself and recording of the attributes.

Is R&D Needed? Not identified

Recommendation: To standardize this practice and to cover the three areas of data source categories (analog, digital and streaming).

Priority: High.

Organization(s): SCC-Accredited SDO

Issue 12 — Data Systems Management

This issue covers data systems management and focuses on managing the systems, including programs, software, algorithms, rules and policies, that manage data. Interoperability and security (with respect to information technology security) were explored. There is a need for standards in the dimension of encryption and access controls relating to security. Standards in the encryption process, tagging of data and authentication of data were explored. There is a need to make sure the quality of data can be guaranteed through security.

The importance of intercommunication between mechanisms and devices to ensure interoperability of data was also explored. It is important to address an element of minimum requirement to load data into a system. There should be minimum standards to meet the requirement of different systems. In addition, data systems management also relates to the lifecycle of the system with respect to the design, development, testing, implementation, maintenance/support and retirement of the system. Data systems management also relates to different types of systems, such as aggregation, data management and data collection, rather than different types of data. It is imperative that governance strategies and governance rules be developed for the systems that deal with data.

It is important to clarify whether the data system management would depend on the type of data sitting in the system and whether there is a need for different sets of standards to address this matter. For example, data systems management could be classified as an application system that ingests, manipulates and deletes data. There is a need to determine if standards are being followed to all the operations or steps of the data lifecycle.

Gap: Data Systems Management. After review of the standards research results, most elements discussed in this issue seem to represent a gap. Results of the research were mostly linked to data management as opposed to the real object of this issue: data systems management. Multiple standards cover data access management. The keyword "Information System Management" gave results that seem in line with the scope of this issue, however targeted to specific fields (e.g., public sector, air traffic). This returns us to the question in the issue description: Would the data system management depend on the type of data sitting in that system? Is there a need for different sets of standards to address this? No standards relate to the data system lifecycle or data system governance strategies.

Is R&D Needed? None identified

Recommendation: To standardize the ability for systems to communicate between mechanisms and devices. It is important to clarify whether the data systems management would depend on the type of data sitting in the system and whether there is a need for different sets of standards to address this matter. For example, data systems management could be classified as an application system that ingests, manipulates and deletes data. There is a need to determine if standards are being followed in accordance with the operations or steps of the data lifecycle.

Priority: Low.

Organization(s): DAMA international

Issue 13 — Discoverability of the Data

This issue covers the discoverability of data, which refers to knowing what data sets and sources exist, how to find them and how to use them. For example, in terms of attributes and metadata, having the information required to later make a fitness for use assessment in programs or activities. An important element for data discoverability includes the notion that the ability to discover data does not guarantee access to the data. The current framing articulates a similar point; access to data does not guarantee its availability for "capture and use."

While data processing, analysis, linkage and interpretation fall outside the scope of the issue of data discovery and access, the role of data inventories or catalogues in facilitating data discovery should be considered in the framing of this issue. It is important to clarify whether there should be a registry or retrieval system and whether the way in which these retrieval systems are set up should be addressed by standards. Determining how to incentivize for people to put content in and maintain these systems was also explored. The potential need to propose a standard to develop taxonomy to categorize available data was also addressed in this issue.

The importance of knowing how data is interpreted, digitalized, captured and put into a format was explored. Keeping track of how data is interpreted and analyzed is paramount for data linkage. Security must also be addressed in relation to the discoverability of data so as to determine which data should be discoverable and which did should not be discoverable. Accordingly, the management of access rights and privileges should also be addressed as there is the possibility for metadata to be protected by being in one system and, from there, stripped and used as real data somewhere else. Metadata is a stage in the data lifecycle where it can morph into data as it moves. There is a need to determine the interplay between privacy regulation and data discoverability. Data must be discovered for regulatory or legal reasons; however, there needs to be privacy protection, such as passwords, around the data discoverability. For example, the case of journalists in war zones and how their pictures can be taken and used by different actors can be addressed by data discoverability.

The lack of clear and consistent definitions needs to be addressed in standards surrounding the discoverability of data. This is particularly true for metadata as it is also a word used to describe the attributes of data being collected. For example, a weather station standard being developed by CSA describes the attributes of weather stations, such as sensors, data transmission methods, frequency and quality management systems around data collection and transmission, to ensure users have an understanding of what they are getting in terms of data as they understand the attributes of data collection. In addition, existing standards and the needs of standards may differ depending on the type of data. For example, it is not clear if there are open standards to address the specific and proprietary ontology of search engines like Google and Apple. Conversely, in terms of ad hoc geospatial creation, the promise of upcoming data does not yet exist; however, its structure is known before it is created. Machine learning or AI for data discoverability was also explored. It is important to determine whether there are best practices, search tools and discovery tools from which we can learn to address automated data discovery and algorithms using AI, ML and APIs.

Gap: Discoverability of the Data. The standards research produced more Tier 1 and Tier 2 results – 45% – than other issues discussed by the working group. Some of the results touch elements that overlap with other issues: for example, data access and security, covered by Issue 21, and metadata and the use of standard taxonomy, covered by Issue 41. In terms of making metadata available for discoverability of data, or in terms of the metadata itself, there are some standards that are either format or language specific and others that are industry specific. There seem to exist a few generic standards towards data discoverability, for example IEEE 2413 – An Architectural Framework for the Internet of Things (IoT), ISO/IEC 19763-1 – Information technology – Metamodel framework for interoperability (MFI), or ISO/IEC TR 20943-1 – Information technology – Procedures for achieving metadata registry content consistency. These standards should be studied to determine whether they cover the elements raised in this issue or if there is a significant gap that needs to be addressed.

Is R&D Needed? None identified

Recommendation: To standardize the way in which data retrieval systems are set up, including a taxonomy of existing data. The importance of knowing how data is interpreted, digitized, captured and formatted is key as it relates to how data is interpreted and analyzed for linkage purposes.

Priority: High.

Organization(s): SCC-Accredited SDO

Issue 14 —
Data Linkage

This issue covers data linkage, which consists of combining information from a person or entity from two or more sources to create a richer dataset. Data linkage addresses the elements of consent and security, as the data does not reside in the same place and, from the privacy side, there are advantages. From the privacy side, data linkage is more of a concept model to fit needs. Semantics, metadata and ontologies are important for data linkage as there may be metadata and logical groupings into domains.

The ethics of data linkage relates back to the original purpose of collection. Linkage may not be for the original purpose of collection, hence the desire to "link" data, and in such cases where the linking of data is outside of the purpose of collection, there are privacy implications. When linking unrelated data points, a person can become quite identifiable. As such, there must be a good purpose stated and formalized to ensure data linkage is being done for a very specific purpose. There is a need to clarify that data linkages are not officially organized data within organizations. Accordingly, there is an option to record linkages as well as linkages where there is information concerning people and then aggregate the information. Data linkage, in the framing of this issue, refers to the general sense of linking of two files. The difference between data linkage and data lineage, which refers to the idea to establish the width, meaning and processes of data, was also explored. There is a need to explore the boundaries between ethics and data linkages to determine what standardization needs to be developed. Additionally, there is a need to determine how ethics relate to governance and purpose for linkage. In terms of the mechanisms, the relationship with the ethics aspect and sensitivity of data linked needs to be addressed, particularly as it relates to identifying whether different mechanisms need to be considered depending on the sensitivity of the data.

The link to aggregation and bringing data together requires standards and guidelines to address both the philosophic and technical side of this issue. There must be some assessment of the quality of the data linkage. The protection of original data, elimination of original data, and ethical concerns around data linkage must be considered. For example, data collection could be dealt with at the beginning rather than in aggregation. Determining how to control data quality coming from data citizen science or different platforms is imperative in contributing to data quality. Given the concerns with semantic interoperability stemming from format inconsistency and inconsistent interpretation of data linkages, it is important for data linkage to contribute to data quality. There are no overarching semantic ontologies. There is a gap in concept models and a fear of having to adapt a concept model, as working on the concept model has some risks.

Gap: Data Linkage. Standards research for this issue produced the most results. Unfortunately, the vast majority of these results overlap with the scope of other issues and do not relate to the specific context described above. For example, citations related to data attributes, semantics and data quality discuss these elements in a broader context than the specificity of data linkage. The element of consent, sensitivity and privacy are well described in a standard relative to health data. The Technical framework of personally identifiable information handling in Internet of things environment seems to cover these aspects as well. Aside from the health sector, there seems to be an important gap in standards relative to data linkage. It should be noted that in 2017 data linkage was addressed in Saskatchewan with Bill 87 – The Data Matching Agreements Act.

Is R&D Needed? None identified

Recommendation: To standardize the practice of linking data while adhering to and addressing privacy implications. Data linkage creates an ethical dilemma and goes beyond the original purpose of the data collection process.

Priority: Medium/Low.

Organization(s): SCC-Accredited SDO

Issue 15 — Manual Tagging of Data

This issue covers the tagging of data where data is abbreviated to specific codes and standardized. Coding standards as they relate to social media, among other sources, was explored. Facial recognition is an important element for this issue. As AI systems use different algorithms compared to humans' way of thinking, manual tagging would correct errors by the AI and override automated algorithms. Accordingly, a combination of AI and corrections made by humans gives much better results than AI-only or human-only tagging methods.

There is a need to clarify whether there are any existing standards regarding rating systems for tagging or any best practices to increase confidence. With respect to the manual tagging of data, a recent news article reported that China is proposing a NWIP[17] at ITU for facial recognition; the article revealed that participants in those committees from the EU and USA are upset about the volume and scope of the standard. There is a need to address this issue as it relates to single entities owning the process of defining a subtopic of metadata. The tagging rules need to be clarified and determined. For example, when classifying data, with respect to the rules for classifying sensitive data, there is a need to address the boundaries of classification to ensure that data can be tagged appropriately. Additionally, smart devices in homes that are collecting information unsupervised and transmitting it to holding areas/companies were explored in the context of this issue.

Gap: Manual Tagging of Data. This issue had the fewest results, likely because it pertains in the most part to more recent technology such as AI, facial recognition and social media. Only 27 standards were identified as Tier I or Tier II. Eleven of those were linked to the keyword "Data Quality Control Assurance" and cover generic data quality management considerations, hence overlapping with Issue 47. However, a few standards seem to provide guidance for important elements of the issue description, such as classifying sensitive data (ISO/IEC 19790) and tag-based solutions to be used in social media analytics (ISO 19731). The standard "Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence – First edition" (ISO ISO/IEC TR 24028), which was released in May 2020, also provides guidance in the selection/creation of training/testing data sets to avoid bias. In summary, there are existing standards that cover items raised in this issue, but some gaps remain, especially regarding new technologies such smart devices which collect a significant amount of information. New systems are prototypes; humans remain involved in the testing of the automated systems. However, given that some algorithms can detect and code information more accurately than humans, how should humans play their role to detect biases?

Is R&D Needed? None identified.

Recommendation: To standardize the practice of manually tagging data to create a diverse approach of reducing errors created by automated systems. The lack of a consensus approach gives rise to bias.

Priority: High.

Organization(s): SCC-Accredited SDO

Issue 16 — Metadata Management

This issue covers the collection, nomenclature, management, accessibility and viability of metadata. The scope of this issue is unclear, as metadata is collected and managed in a range of contexts, including in structured datasets/bases and on the web. There are also different types of metadata such as descriptive, structural and statistical, among others. Metadata management involves developing, adopting or adapting a schema, which consists of the 'meta' data elements or attributes that contextualize a dataset/base or other digital resource.

[17] New Work Item Proposal

Data is often created using a variety of technical processes. As assessing fit for purpose determines whether data is right, metadata management can assess whether data is trustworthy. Metadata is relevant in documenting the purpose and the quality level for that purpose. To avoid duplication, considerations of quality should be focused on metadata, not data. While the assessment criteria for both overlap in many ways, they should be distinct in the framing of the issue.

Security safeguards were also explored in terms of the access to data management collection. Some metadata itself is confidential compared to data. The aggregation of data changes metadata management, as access controls and who is accessing, touching and seeing data need to be considered. With respect to the relationship between metadata and security safeguards, metadata can be used commercially and can be very valuable. There is the potential for metadata, as it relates to security safeguards, to lead to ethics issues, such as rules for sharing metadata, and security issues. However, PIPEDA safeguards can be addressed in relation to these ethics and security issues.

The importance of quality of metadata and its relativeness to what data is was explored. Marketing research data may have much higher tolerance for errors relative to metadata than medical equipment. Therefore, the same level of quality cannot be applied to all data. There is a need for a clear definition about where metadata begins and data ends. Metadata is often defined as data about data, which is not very clear. Data lineage, which is all processes the data goes through, is important as there are different types of metadata, such as technical metadata and scientific metadata. Others refer to three types of metadata: operational metadata (basis for data governance); technical metadata (lineage information); and business metadata (details of processing and accessing the data). In addition, the issue of metadata management is strongly linked with data discoverability, fitness for use, data quality and data collection. It is recommended to consider existing metadata schemas – for example, Dublin Core's Metadata Element Set, Open Government Metadata Application Profile – in the research and gap analysis for this issue. The Treasury Board Standard on Metadata can be consulted for more examples on relevant and widely adopted standards in this space.

Gap: Metadata Management. While this issue covers a broad range of elements which are not all clearly defined, interesting results were obtained by the standards search. Most key elements of the issue description, such as metadata collection, nomenclature, access, security, semantics and ontology, seem covered by separate standards. Metadata collection seems particularly well covered. The standards ISO 23081-1/23081-2 seem to cover a broader range of elements covered by this issue, namely creation, capture, maintenance and access. The first ISO 23081-1:2017 "Information and documentation – Records management processes – Metadata for records – Part 1: Principles" is a principles-based standard which links requirements for metadata to the core professional statements in the foundational ISO 15489-1. The second ISO 23081-2:2009 "Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues" is a practical approach to implementation, providing discussion on implementation options, managing metadata and a conceptual model for defining metadata elements for records. There are two caveats worth noting. First, generic standards on semantics and metadata systems do not seem to exist. There are, however, industry-specific standards for these two elements. Second, there is no mention of data lineage in any of the standards found, meaning complete metadata on all processes the data went through might represent a gap.

Is R&D Needed? None identified

Recommendation: To standardize the terminologies around the management of data about data.

Priority: Medium.

Organization(s): National, regional or international SDO

Issue 17 —
Organizational Data Policy Strategies and Risks Management

This issue covers data policy strategies and risk management, recognizing that these can vary across industry. The potential inconsistencies, which can make data policy strategies and risk management more complicated, were explored. Data policies can be focused on certain things and rely on other policies that have data-related requirements. Organizational data policy strategies need to analyze and integrate a lot of different data sources. Accordingly, departments and organizations should have policies related to integrating data. Data portability, as the extent to which the owner of the data has control over data, was explored.

Risk management associated with the sensitivity of the data regarding aggregation, privacy assessments and de-identification strategies was also explored. There are risks associated with the policy framework itself. The Government of Canada Digital Charter seems to be a prime example of risk management. There is a need to ensure compliance to policy through levers. There is a strong association with the governance piece in terms of access and controls.

Gap: Organizational Data Policy Strategies and Risks Management. Multiple standards were identified as a result of the research for this issue. Standards regarding data governance, accountability, rules, data policies, data protection and data portability exist. They can relate to various contexts: AI, cloud computing or specific sectors and data types. These standards should be studied to determine if they are consistent and if there is a need for a more generic standard or if these standards cover all the elements of this issue. It is not clear at this point if levers to ensure compliance are discussed in these existing standards.

Is R&D Needed? None identified

Recommendation: To standardize the approach of creating organizational data policy strategies and risk management frameworks.

Priority: Low.

Organization(s): National, regional or international SDO

Issue 18 —
Data Quality and Fitness for Use Assessment

This issue covers the consistent reporting of data quality in terms of what metadata is collected consistently to ensure quality of data. There are multiple definitions of data quality, using dimensions, usually between five and 10. The definitions of these various dimensions all cover the same concepts. Among these dimensions we find relevance, coherence, timeliness, accuracy, completeness, consistency, accessibility, objectivity, readability, uniqueness, usefulness, accuracy, interpretability and reliability.

There is a need to address the frameworks to put in place with respect to the quality process, and how to measure the quality. Accordingly, good practices must be determined and adopted to ensure these frameworks are implemented. There should be an element of responsibility, accountability and authority attached to this issue. In addition, this issue determines the level of quality as the outcome of data profiling. Due to the associated cost, the step of data profiling is at times skipped. The notion of profiling in the lifecycle should be a mandatory step, as without data profiling there is lack of awareness of data quality. There is a need to determine what at a minimum defines quality data and how this can be measured. These answers are very dependent on the type of data discussed. The notion of time is important as there are questions whether the passage of time changes the quality of data since its collection and whether the data remains relevant. This is included in the timeliness dimension.

Data quality as it relates to the lifecycle process, the quality of the input, the process and the output was also explored. In ongoing work to develop a federal data quality framework, quality is identified with fitness for purpose, recognizing that some dimensions of quality will be ‘internal’ to the data, pertaining to characteristics of the data, while others will be ‘external’, pertaining to the use to which the data is put. Dimensions are sometimes classified based on whether they are subjective or objective, a similar but potentially confusing approach. Quality is also linked to fitness for use, meaning quality is relative to the user’s needs; however, its assessment is based on objective measures or indicators. These measures or indicators can be qualitative or quantitative and need to be identified prior to the assessment exercise. Among the quality elements to consider, the source of the data must be considered to determine whether it is reliable and an authority in the subject. Given the limited scope, the focus remains on the description of datasets and methods used to create and collect data. This description must be clear to ensure users can make determinations of fitness to use. Creating the metadata on the data, data attributes and rating systems needs to be a focus. There is a need to be careful with a rating system, particularly if it leads to a single score at the end, as not all quality elements have the same relative importance to all users. This issue is linked to metadata management.

Gap: Data Quality and Fitness for Use Assessment. Many results obtained for this issue are citations from the ISO 8000 standard on data quality. While it may not be applicable in all contexts, this standard is a strong foundation for data quality management. Other standards target specific industries, in particular metrics to use to measure data quality. Various references have various data quality dimensions and definitions. Is there a need for a standard definition of quality? If so, this is a gap. There is one standard on geographic information that explicitly describes the importance of metadata to allow for fitness-for-use assessment.

Is R&D Needed? None identified

Recommendation: To standardize the frameworks put in place to understand, describe, measure, monitor, verify, attest and report on data quality.

Priority: Medium.

Organization(s): National, regional or international SDO

Working Group 3: Data Access, Sharing and Retention

Issue 19 — Consent Management (Consent, Access and Withdrawal to Data)

The scope of his issue covers aspects of consent as they relate to data access. Consent Management can be described as a process that allows a system to meet privacy regulations by obtaining user agreement for collecting a subject's data. While consent is obtained at the data collection stage, this issue focuses on consent in the context of accessing and using the data in real time. Visibility needs to be provided to the subject on who manages consent so they may have access to all the agreements they have signed. "One cannot withdraw data if they do not know where to withdraw from." Mechanisms need to be in place to guide the subject and provide awareness while granting data. Further discussion around granularity of consent needs to be conducted to determine what portion of data does the subject consent to. Identity of the subject is not just the person but also unique data identifiers. Out of scope subject matter for this issue includes:

- Consent Management of entity, which will be dealt with in another issue.
- How data is stored as it relates to Electronic Health Records, Data Trusts, Personal Online Storage, etc.
- Broad principles – residency, purpose, recipient, granularity – and bigger concepts that could be codified into future standards.
- Any changes to data stored would need to be tracked as well on the dynamics of the consent itself.

Consent has many facets that provide for a complex approach to defining the mechanisms that will govern how a subject agrees to giving away their data. With distinct perspectives on how data should be accessed, there is a need for a common language to help ease regulators, innovators and consumers in their conversations. There are many published and proposed definitions, but there is a lack of consensus and a poor understanding of the adoption of these terms. Describing data access would be useful for this issue, as individuals give consent to multiple platforms, to understand who and what they are giving away. In addition, the concept of consent begs the question whether it is a contract to forgo your personal data. Individuals alone are responsible for multiple services they consent to; hence the need for a tool that is designed to provide that type of service to an individual. The development of a standard for transferring consent would be an ideal scenario for this issue. Consent has to be informed and details on data usage need to be provided; otherwise, individuals do not know what they are consenting to.

There is a need to create a level of trust mechanisms through which consent can be granted without having read the fine print. Individuals need to trust the system and feel that custodial and stewardship of data innately exists. This concept is difficult to define and codify, but standards around such mechanisms are very important. Defining trust in the context of consent is an avenue that standardization can explore to alleviate the gaps of this issue. The Pan-Canadian Trust Framework utilizes a set of rules and tools designed to help enable trust in the system, but nothing out there addresses the ability to put trust in an entity to use your data in an ethical manner. Standards could explore ways to enhance use of data and allow for data use that goes beyond consent by defining what that context is with a level of aggregation and assurance.

Gap: Consent Management (Consent, Access and Withdrawal to Data). According to the seven guiding principles for meaningful consent provided by the Office of the Privacy Commissioner of Canada, individuals need to understand the nature, purpose and consequences of what they are consenting to. In order for consent to be valid, or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner.

Based on the triage analysis, this issue generated a significantly high number of standards related to data consent, data access and consent to withdraw data. The standards generated by our search address topics that are crucial to the issue and are up to date to reflect the unique aspects of how data is collected today. Due to the recent increase in commercial value of data, the practice of collecting and storing large amounts of data has called for further standardization activities to address errors in the consent validation process and non-compliance.

As technology evolves, the lawful processing of personal data gets skewed, hence the need for succinct standards in the consent management space. The standards reviewed in the triage analysis do not address machine-to-machine consent or mechanisms that enforce how consent is granted through the whole data consent process; these are areas where further research could assist. Other areas of consent management where gaps exist are classification of depersonalized data and digital identity.

Is R&D Needed? Yes (Classification of depersonalized data, Primary/ Secondary Use of data, Does the recipient of the data need be identified?)

Recommendation: To standardize such agreements and how they cover either a specific data item (fine grained) or a broad range of data topics (coarse grained) either acquired in the past or expected to be acquired in the future. Also, how the digital forms of such agreements are managed throughout their lifecycle; whether and how they accompany each data transfer and exchange; and how their withdrawal may impact the data already shared.

Priority: High.

Organization(s): DIAAC, W3C, Office of the Privacy Commissioner of Canada

Issue 20 — Data Access

By 2021, there will be nearly 4.5 billion global internet users generating over 3 ZB of data. How does one find their way to the right data repository and, when the right data repository is found, how does one gain access to this data securely? These are questions that might be able to be answered by standards. Finding the data will be the issue; therefore, standard definitions are required for role-based access controls to data repositories or standard metadata for classifying data by sensitivity level (and determining access that way).

The scope of this is an overarching issue for WG 3 that covers several aspects of the process to provision access to data to authorized individuals. How do we further define data access for the purpose of this issue to create a better framework? This issue also addresses semantic access to data.

In scope:

- Types of Data Access (Random vs. Sequential)
- Process around data access – a step-by-step way to access the data. Before even accessing the data, you need to know if the data is fit for use in the analysis you are doing. Issue 27 is also talking about access to metadata, which is a key element of this issue.
- Data Query and Searching
- Ease of use/clarity around steps required to access the data (i.e., you should not need to be an expert in order to access the data). This can be facilitated by metadata – knowing what the permissions are to access the data. There could be a standard around requesting permission to access the metadata. Create principles around the process of accessing data (i.e., all steps are listed out).

- First element – specifying the data set (data query, SQL, etc.).
- Second element – contract between data consumer and provider about how that data set will be extracted, what the purpose is, time value, etc.
- Third element – controls. Once permission is granted, where does one go to take control over the data connections (i.e. deleting connections, changing permissions)? The ability to revoke data access.
- Access to datasets for exploratory analysis. Story and contract around how datasets are accessed.
- The purpose of data access. Data users has the obligation to specify the purpose of data use.
- Restrictions and policies – what kind of standard can be used so data providers can put restrictions on the dataset that is being provided (destroyed after first use, not sent to third parties, time values)?

Out of scope:

- Data discovery (Data Access is more around the permissions/ security/ roles) – some elements are in other issues (Issue 52 for data tagging and traceability) but discoverability has not been captured.

Creating a layer that "knows what's out there" is required (i.e., finding things requires Google or other search engines). Need to be able to easily identify what data is out there. Facilitating the finding of relevant data sources in a standardized manner. Today we are struggling to find where good data is. For example, to facilitate right of access to information, legislation was made for a tool for publication that standardized how Government institutions presented their data sources. This is a necessary piece to make right-of-data access effective and mandated in the Access to Information Act. The descriptions had to have the same elements to make it "standardized." WG 2 discoverability and accessing metadata.

There a need for standards to address data access in the context of understanding who gets access to what data, with a framework that makes it easy to understand what process to follow. Furthermore, the ability to retrieve personal data for it to be erased is vital for this issue. Other topics for exploration where standards could provide clarity include:

- Ease of use and transparency around access to data; however, standard lies within data discoverability (issue lies with WG2).
- If a consumer wants to access a data set, he will need to access it by means of a query. The ambiguity lies within what is the data, what is the time frame of access – this is where a data access standard piece comes in (query and contract). The contract sets parameters for the consumer on restrictions to data.
- Imposing restrictions on the consumer with regards to access to what you need/purpose of data access or request?

Gap: Data Access. Based on the triage results generated from the standards search, a large number of standards were deemed irrelevant to this issue. Most relevant standards appeared to be broad in scope, addressing topics such as access controls and privacy by blockchain design. However, these standards did not address topics such as data access controls in relation to big data and the facilitation of artificial intelligence and machine learning.

Big data presents challenges when addressing data collaboration, and the need for research and new standards to address this gap is vital to enable better data access.

Is R&D Needed? Yes – Data access controls tailored for big data, Data Links, management of permissions

Recommendation: To standardize how data providers and data consumers establish and negotiate data access contracts with usage policies that are both machine and human readable, and therefore interoperable. Also, how these contracts with their restrictions and obligations are being enforced during data retrieval and further along when the data has been delivered to a data consumer.

Priority: Medium.

Organization(s): ISO/IEC, BSI

Issue 21 — Data Retention

The scope of this issue covers what standards need to be created to provide a procedure within an organization for retaining information, beyond personal data. A robust data retention approach should detail how long data is stored and how to make exceptions to the schedule in the case of lawsuits or other disruptions. The development of a framework should address these components:

- Determining data storage period and providing information to individuals on retention period
- Business need or reason to keep data (privacy versus economic concern)
- How and why is data being collected
- Option to opt out/in
- Organized data for future use
- Disposal of data that is no longer needed
- Right to be forgotten

Depending on the industry, data retention schedules may be guided and determined by regulations under which those industries operate. Use cases become important in this regard; the general recommendation by the industry is to include a data retention map within their policies. Retention should be a specific date or an event (i.e., 30 days after a webinar) with the element of disposition (removing everything related to a certain subject). Data lifecycle management helps review the amount of data being held and transfers it into something usable for the future in not an exact form of the original. There should be a specification of how the data is securely stored, with a process of how it is archived into something else. Data security standards applied to active data should be applied to retained data.

Data classification is vital to this issue. The differentiation between personal, critical, primary and public data play a role in how this data fits into a retention policy. Furthermore, entities need to ensure the structure of the data is retained as well as the data itself. The retention schedule may need to be modified based on the ability of the database to have the data removed without breaking it. It is worth noting that proprietary format and media may cause issues in usability in 10-15 years, due to changes in technology. Privacy commissioners should be careful that the data structure is not used as an excuse for data not being able to be removed. Policies in the Ontario Public Service address this subject, especially for legacy systems. This allows data retention to be moved to the decommissioning of the system as opposed to an event or certain date.

There is a need to determine how regulations will come in to play as far as data retention is concerned and what kind of practices can support long-term data retention. As the commercialization of data creates rewarding business models, the storage of personal data after it has been collected requires informed decision making on how long to keep it and when and how to dispose of it. There is a temporal dimension to data retention, only for short period of time given; how long you have to keep data in certain industries would be different; have to assess at an industry level. Other areas that require further research on best practices are the right to forget and open banking, where the consumer owns their data and the vendor has to gain their permission.

Retention regulations could direct specific data protection, but data protection standards should be a separate category. As data governance experts have tried to tackle the data retention piece for a while, the focus should be on the “net new,” i.e., significant amounts of data being used from IoT devices is being aggregated and used but a lot of the original data may be lost. Data transfers, data exchanges and portability are in scope for this issue.

Gap: Data Retention. The standard search related to Data Retention generated a high quality of standards that address topics such as the right to be forgotten, data storage limitations and disposal, records management and data archiving. These are key topics within data retention. A conclusion can be made that this Issue has gained high visibility among standardization networks and regulatory bodies, leading to the creation of best practices around data retention.

The standards search reveals that guidance documents have been made available to tackle questions around entities that collect data with the intention to use it for purposes other than originally intended. New data custodians have limited regulations governing how long they can retain data. There is currently no single standard addressing new data-hosting entities.

In conclusion, the initial research carried out determines that there are no gaps within this Issue, but further research might be required to ascertain this conclusion, especially when it relates to data custodian jurisdiction.

Is R&D Needed? Yes. Sector-specific data retention standards (each sector has its own regulatory requirements for holding data; e.g., banks store data for 7-10yrs).

Recommendation: To standardize how to express retention rules and policies that will govern how data custodians manage the lifecycle of data including archiving, transforming, compacting and decommissioning data in their repositories in a way that is secure, transparent, portable and compliant. This should also include aspects of discontinued data formats and tools that, if not handled properly, might render retained data unusable.

Priority: Medium/Low.

Organization(s): Office of the Privacy Commissioner of Canada

Issue 22 —
Identity Management – Validation and Authentication (People, Entity & Devices)

The scope of this issue covers the specific terminology and concepts for identity management (IdM), in order to promote a common understanding. Identity management describes the management of individual identities, their authentication, authorization, roles and privileges across boundaries.

Customers have made it a common practice to maintain user accounts with different service providers to access a range of services. In such environments, all attributes of the identity must be verified to operate, otherwise the resources would be vulnerable to data loss. Identity management is a framework of policies and technologies for ensuring that the proper people have the appropriate access to technology resources.

The current data governance framework needs a standards solution that can address digital credentials as they relate to identifying persons. Digital identity helps address identity management shortcomings by allowing for information to be assessed and authenticated through an online business system without the need of human operators. Areas for further standardization exploration include cryptographic credentials and identity networks.

Gap: Identity Management – Validation and Authentication. A strong data governance model requires an Identity Management system that provides an added tier of protection by ensuring data access policies and rules are applied consistently across an organization.

Based on the triage analysis done for this issue, most standards were relevant to Identity Management and its attributes. The identified standards cover topics such as cryptographic credentials, multi-factor authentication, use of biometrics, digital wallet and identity. As technology evolves, authentication methods will need to evolve at the same pace to stay relevant. Further research to assess whether emerging technology such as AI and ML hinder or improve validation and authentication methods might be needed. Some sources have inferred the notion that AI and ML are the new brain of identity and access, where fluid responses are needed to address threats rather than firewalls. These could be questions that are posed to DIACC for support through the Pan-Canadian Trust Framework.

Is R&D Needed? Yes, how will artificial intelligence and machine learning affect identity management? Will these technologies hinder or improve validation and authentication methods?

Recommendation: To standardize the way digital credentials are issued, used and managed so that the actors they identify (persons, organizations and devices) can securely participate in data transactions. This includes federation and authentication across identity networks both for the purposes of adherence to data access policies and restrictions when exchanging data as well as for identifying who participated in past transactions.

Priority: High

Organization(s): SCC-Accredited SDO, DIACC, Canadian Centre for Cyber Security

Issue 23 —
Data Sharing, Exchanging and Integration

The scope for this issue will cover the governing principles around the sharing, exchange and integration of data. It is important to note that each topic carries elements of data privacy that need to be understood to provide clarity accordingly in the data governance model. Establishing relationships between different data sources is key to this issue. Areas mentioned below are vital to defining the scope of the issue:

- Technical delivery modes for data exchange
- Encryption methods
- Standardized language for data-sharing agreements
- Data-sharing impact assessment process

Data Exchange occurs between two parties and is a bilateral agreement. The focus is around the agreement of exchange. There is a need to determine how the share, exchange or integration of data from various jurisdictions should be governed. This issue will focus on the outcome established by the decision to integrate various datasets, with or without consent. It is noted that the management of bias is necessary to capture the right outcomes and there may be a greater need for transparency when addressing the outcomes.

Data Sharing is defined as the ability to share the same data resource with multiple applications or users without being changed. Broader exchange is multilateral, with a range of consumers and service providers. The agreement is implicit in the essence it is shared. Once data is shared, how do you know or mitigate transparency around its further use?

Data Integration is defined as the interpretation of the data by the receiving party. There is a need to understand the relationship between parties with regard to integrating different sources of data.

The unknown elements that happen during the process of data sharing, exchange and integration lead to determining what policies need to be employed. For example, when you share data, you do not create a copy; a copy is created when it is exchanged. What happens on the other side cannot be managed or controlled. Risk associated when exchange of data is stored in a cache is unknown. For example, patient-gathered data used for purposes outside original collection.

Gap: Data Sharing, Exchanging and Integration. As the value of data becomes greater, the arrangement/contract of sharing, exchanging and integrating information becomes a dilemma. In a rapidly evolving data ecosystem, data custodians are finding it difficult to manage the collaboration of data between consumers. The triage results can attest to this, as most of the standards analyzed for this Issue were categorized as irrelevant or sector specific (signal transmission for utilities, telecommunications and transport). There is a need to create a standardized language for data sharing agreements or frameworks, with focus on the contract itself, which could include a data sharing impact assessment process to help address the gaps in this issue. For example, the Singapore Trusted Data Sharing Framework outlines three general models of data sharing (bilateral, multilateral, decentralized) as a facilitation method to guide the data-sharing journey. The clarity needed is the standardization of contractual aspects, not the technical language.

Is R&D Needed? Yes. Further research is required to determine which key areas require prioritizing to create the foundation for data collaboration.

Recommendation: To standardize the data-sharing agreements and/or frameworks with focus on their contractual rather than technical aspects, including all types of data-sharing and exchange scenarios (bilateral, multilateral and decentralized) as well as data integration – when data is embedded and becomes an integral part of another asset (a product, a service or aggregation).

Priority: Medium.

Organization(s): SCC-Accredited SDO, C4DC (Contracts for Data Collaboration)

Issue 24 —
Trusted Data Intermediaries

The scope of this issue will assess how data intermediaries provide independent, fiduciary stewardship of data. The scope will help understand how an Intermediary governs data and determine the implications of improper withdrawal of data and data use authorization. There is a need to develop standards that Trust Intermediaries should adhere to, with a focus on the intermediary rather than the repository. Is it feasible as part of a data governance framework to have a data trust that manages data only as an access portion? It is vital to have standards that oversee entities that store data between parties, to stay independent and act fairly.

A data intermediary is by definition a broker of data, but its core function as a data intermediary needs to be explored further. A data intermediary needs to be a minimalist by nature, although there are cases where some intermediaries take on other functions. An intermediary performs several roles depending on where it is in the data lifecycle, hence the need to address an intermediary's roles as it takes on a different role through the data lifecycle. For an intermediary to qualify as a Trust, it needs to adhere to multiple standards to demonstrate certain qualities that show compliance. Some form of auditing needs to be captured through standardization (Intermediary Audit, in case of failure to work within a Service Level Agreement). In terms of trust intermediaries, what are the elements that make an intermediary trusted? Not every organization can claim to be trusted; there needs to be an adherence to a level of cybersecurity and other compliance measures – for example, PayPal brokering the lack of trust between merchant and buyer; digital trust is not an element of the intermediary; all entities need to be identifiable.

The standards used in healthcare, such as digital contracts, allow for traceability to broker transactions, and data subject/owner is viewed as an element of defining the policies of data. Standards can help intermediaries to enforce how data should be handled and further set a minimal set of standards to claim trusted intermediary status. This issue will focus on creation and sharing of data. Data Trusts are created as an approach to look after and make decisions about data, involving one party authorizing another to make decisions about data on their behalf, for the benefit of a wider group of stakeholders. The notion of having trust intermediaries has created a push for trust creation; the governance of these trust intermediaries must be determined and specific standards have to be created for trust intermediaries. This issue also addresses separating data from applications, and the implication of withdrawing data and the authorization to use data.

Gap: Trusted Data Intermediaries. In a Canadian context, the meaning of a trusted data intermediary is not clearly defined. This presents an opportunity for standardization to capture the definition around intermediaries and clearly distinguish between a data broker and an intermediary. Furthermore, the arrangement between intermediaries and the organizations they work with requires better-defined parameters (e.g., level of ownership of data – temporary versus long-term). Trusted data intermediaries have the responsibility to explore how to govern their data through an accreditation/certification process that can establish trustworthy principles, a process for reviewing applicants seeking accreditation, and an established set of practices to be adhered to.

Based on the triage results generated from the standards analysis, very few standards were found to be relevant to the issue. Most of the relevant standards appear to address securing data and metadata rather than the factors that qualify, certify and accredit trusted data intermediaries, the role and level of a data custodian, or lifecycle for metadata and data. It is worth noting that the relevant standards to this issue were published recently and that the standardization ecosystem, especially in Europe, is currently aware of the gaps that exist in addressing trusted data intermediaries. Topics of interest include data unions, a hybrid version of a broker and data intermediary.

Is R&D Needed? Yes. Research is needed around accreditation and certification of trusted data intermediaries. How do intermediaries create an arrangement with other actors as it relates to negotiating usage right, access permissions, licensing?

Recommendation: To develop standards that any data intermediary will need to adhere to for independently storing and/or brokering data between parties and be “trusted” by the ecosystem, and to clarify whether, or under what conditions, such data intermediaries can make decisions on data on behalf of the data owners and how they would comply with any data use contracts set by these owners who may temporarily or permanently transfer data under their custody.

Priority: Medium.

Organization(s): SCC-Accredited SDO

Issue 25 — Authorization for Data Collection and Sharing

The scope of this issue covers aspects of permissions as it relates to who has access to what in relation to both personal and industrial/commercial data and what data policy is in place to protect sensitive information. Industrial data does not have the same consent (authorization) aspects as personal data, hence the need for a granular governance model. Industrial data and the handling of data from one machine to another (or systems) would be difficult to have the same kind of contract as we would have in the commercial or personal level. The contract might be partially in the software or governed by an external contract. The creation of authorization endpoints through application programming interfaces (APIs) could help provide clear authorization endpoints and give access only to certain individual records.

There is a need to address who has the authority to control the collection and/or sharing of data, especially industrial/commercial data. Organizations collecting data tend to overpower their subjects into providing consent without any privacy protections. Industrial data is collected through contracts, but there can be a power imbalance (i.e., small firms do not have same ability on contractual terms for data use, in case they want to leverage that data). Consent to use a product or service is consenting to a contract.

The creation of a standards framework may be a challenge to collect permissions as it applies to passive data collection from IoT devices both in public use and private use, since the data collected may be going to multiple companies or authorities. Furthermore, a governing body needs to be assigned the duties of monitoring and authorizing the collection and sharing of data.

Further aspects of this issue to consider revolve around passive devices that collect data and authorities that have it extracting it for commercial use (e.g., if someone flies a drone over a neighbourhood taking pictures of the number of cars in the neighbourhood, the number of swimming pools, etc.).

Gap: Authorization Data Collection and Sharing (proposed: Authorization for Passive Data Collection and its Further Use and Sharing). Based on the triage results, most standards generated for this issue were considered to be relevant. These standards cover areas such as consumer privacy protection for IoT product usage and guidelines for sharing data extracted from connected and smart systems.

However, in the age of the data economy, a growing number of individuals and third-party and independent entities are recognizing the opportunities and business potential that data provides and seeking data in unfamiliar places. For example, a drone flying over the neighbourhood taking images can commercialize this data to the right consumer. This type of practice requires an authority (governing body) with parameters to oversee such activities to ensure privacy rights are not violated when data is collected passively. Generally, this is where a gap exists in this issue for standards to be developed.

Is R&D Needed? Yes. Legal aspects of this issue need to be explored.

Recommendation: To standardize the policies around data collection and how this collection is authorized, how the authorization is enforced, under which circumstances the collected data can be processed and shared as an aggregate information, and if/when individual data is allowed to be extracted from such aggregate datasets.

Priority: High/Medium.

Organization(s): ISO/IEC

Issue 26 — Encryption

The scope of this issue should also cover the method of encryption and what is accepted by industry/industry-level standards. Encryption provides the means of applying security in the context of data sharing and access but is not the only means of doing so. Other novel ways are being introduced to provide security and privacy in terms of the way information is protected and accessed. This includes the encryption of synthetic data as well. Encryption entails three aspects: data at rest (data repository side); data in transit (sending to another party); and at side of data consumer. Securing data has been challenging in the latter stage of the encryption cycle, but a new method of encryption called homomorphic encryption has established a technique of protecting data when it is provided to a data consumer. This new form of encryption provides data readability to the consumer without revealing specific details of data in the dataset.

There is a need to develop standards that define acceptance criteria for privacy in specific contexts. Furthermore, the lack of standards around the limitations a data consumer has when using data raises questions such as what happens on the data consumer side. How can standards enable the broader use of data while still conforming to privacy and confidentiality rules? Having these types of protections in place helps prevent and mitigate the sensitivities of using that data. Managing encryption over time presents its own challenges, as what is encrypted today can be decrypted tomorrow. Standards cannot predict what new technologies are coming along – for example, researchers believe a quantum computer will have the ability to decrypt any dataset.

From a consumer standpoint, there is a blurry line between personal and public data; there is a need to develop explanations for this blurry line. WG 1/WG 3 address the privacy, ethical use of data and cybersecurity practices component of this issue. If looking at this issue in the context of de-identification, de-identification as a stand-alone issue is addressed in Issue 46. Issue 49 concerning IP should be added to WG 4.

Note the difference between encryption of data at rest versus encryption of data in motion, and encryption of data in analytics.

Gap: Encryption. Based on the triage results generated by the standards search, most standards were deemed to be relevant to this issue. The standardization ecosystem highlights the value for homomorphic encryption with a significant number of guidelines available for use. Further standardization efforts could be focused on defining acceptance criteria for privacy in specific contexts, such as differential privacy and personal versus public data.

Is R&D Needed? Yes. Differentiating between personal (non-identifiable) data and public data. The need to maintain anonymity when data has been acquired.

Recommendation: To standardize the use of encryption and its acceptance criteria for conforming to privacy and confidentiality rules while using data which takes account of the advances that new technological development (such as quantum computing) may bring.

Priority: Low.

Organization(s): ISO/IEC

Issue 27 — Management of Ontologies

In this issue, we explore the need for principal elements (bridge language) that guide the use of sharable and reusable reference terms for the interoperability of data stored in databases. The scope of this issue will cover the management of ontologies (vocabularies, concepts and tools) as they pertain to better data management. This will ensure a common understanding of information, resulting in interconnectedness and interoperability of data while making data invaluable by addressing the challenges of accessing and querying it. Standardization can address how ontology should be defined using a Canadian lens and provide a national ontology registry with governance standards. Ontology models are generally proprietary, hence the need for open rather than controlled vocabulary.

There is a need for managing controlled vocabularies; builders of medical informatics applications need controlled medical vocabularies to support their applications, and it is to their advantage to use available standards. In order to do so, however, these standards need to address the requirements of their intended users. Over the past decade, medical informatics researchers have begun to articulate some of these requirements, such as vocabulary content, concept orientation, concept permanence, non-semantic concept identifiers, poly-hierarchy, formal definitions, rejection of “not elsewhere classified” terms, multiple granularities, multiple consistent views, context representation, graceful evolution and recognized redundancy.

The management of a variety of vocabularies and ontologies (i.e., translation between ontologies) on how to semantically understand the data once you have access and how it was coded is important. For example, when an individual accesses data, they access an encoded concept by a data source, but if they don't have the possibility for ontology source, they will not be able to interpret the data. Ontologies enhance data quality and help make better sense of data. For example, the pharmaceutical industry system (Shoppers and Rexall) may not use the same vocabulary to dispense the same drug. In order to ensure uniformity, they need a similar vocabulary. LOINC (Logical Observation Identifiers Names and Codes) currently serves as a set of common reference terminology for laboratory and clinical observations. A similar reference management system can be created for other sectors.

Gap: Management of Ontologies (proposed: Reference Terminology). Based on the triage results generated from the standards search, the results provided a neutral stance on whether standards were relevant or irrelevant to the issue. Half of the standards were deemed as Tier II (partially related to the issue), whereas the other half were ranked as Tier III (sector specific). After conducting further due diligence, it was concluded that a gap exists, and the issue requires further research to help inform which sectors could use a "bridge language" for interoperable data exchange.

Is R&D Needed? Yes. There is a need for principal elements of reference to serve as a guidance. Reference data management systems (LOINC).

Recommendation: To standardize the management of ontologies (vocabularies of concepts, hierarchies, relationships, etc.) and their lifecycle (from concept definition to discontinuation), as well as their application in describing data and its semantics, including complex coding practices such as post- and pre-coordination, and the way data consumers can get access to the ontology that describes the dataset they retrieve.

Priority: Medium.

Organization(s): LOINC, NCBI

Issue 28 — Data Transparency, Lineage and Traceability

The scope of this issue will cover transparency and traceability of data. As new legislation requirements seek a better understanding of the data lifecycle; data transparency, lineage, and traceability have emerged to be vital elements of data governance/ management. This issue helps to provide better context as it relates to the flow of data, how it is tracked and the ability to easily access it.

By definition, data lineage is representation of the path along which data flows from the point of its origin to the point of its usage. Data traceability is the ability to ensure the tracking, if possible, in real time of activities and information flows linking activities. Given the option, users and data owners track how their data has been used in a complete audit trail, while tracing and maintaining confidentiality. Audit trails should not reveal what data is about but elaborate confidentiality and privacy rights. The focus of this issue will be around the trail of data while its being used through its lifecycle. Data tagging is out of scope for this issue.

Standards to provide a mechanism of creating relationships between a new piece of data and the piece of data it is referenced to (relationship between the data tag) would allow data owners and users to understand where data comes from and how it is used, hence, understanding the data value-chain.

Standardization could clarify questions arising about the meaning of transparency on metadata, such as, "does transparency extend to the algorithm used to gather that data?" (e.g., data from a client in the banking industry can be derived to provide further information – does transparency get extended to the derivation used to alter the data collected?)

In addition to the transparency challenges mentioned, below are a few more examples that can be supported by standards framework:

- If a data provider sends data to a data consumer, we create a transaction. If the consumer transforms the data and shares it with another consumer, it creates a separate transaction.
- If data has been used and the original data owner withdraws it, we can assume that it is an artifact. We need a level of transparency to the withdrawn data.

Gap: Data Transparency, Lineage and Traceability. Based on the triage results generated from the standards search, most standards were deemed to be very limited in scope and would only be useful to specific sectors.

Further research is needed to address topics such as data validation, data audit trail, creation of a data value chain, data actors and derived data traceability that would elaborate on the different aspects of the data journey as it relates to the issue.

Is R&D Needed? Yes. There is a need to address data value chain, derived data traceability, traceability around blockchain, Internet of Things, Digital Identity, chain of custody, RACI matrices.

Recommendation: To standardize what information needs to be captured about a data item when it is acquired, exchanged, modified and used as a source for other data creation or analysis; who can access such meta information and under what circumstances; how this meta information should be protected, retained and disposed of, independently of the data item it describes.

Priority: Medium/Low.

Organization(s): ISO/IEC, DIACC

Issue 29 —
Data Portability and Mobility

The scope of this issue will focus on the creation of a framework that ensures interoperability between systems enabling the user to be in control of their own data, due to the lack of categorial structure for data elements and the ability to extract data in digital form, and preserving the exchange of information without it being explicitly transformed to provide the same kind of usability.

Data portability and mobility requires common technical guidelines to facilitate the transfer from one data controller to another, for example, device portability from one cellphone to another. The right to data portability allows data subjects to receive personal data they provided to a controller in a structured, commonly used, and machine-readable format, in addition to providing the ability to transmit that data to another controller. The goal is to provide a framework that allows for the export of data in a detailed structure, while maintaining the ability to provide context and dictate where data can go without it being massaged by an individual to allow it to be used.

The need for preservation of information exchange between systems so that it can be utilized in more than one system/machine without it being explicitly transformed to provide the same kind of usability is vital. For example, in the case of consumer-directed finance, portability and mobility serve as a gateway for many new financial management digital services to consumers as it relies on access to consumer financial data. There is a need to provide a distinction between portability and mobility, as mobility could affect the usability of the data.

Gap: Data Portability and Mobility. Based on the triage results generated from the standards analysis, most standards were deemed relevant to the issue. One key finding in the standards search was that most of the standards were developed recently, an indication that standard developers are addressing the gaps in this issue. Further research could help alleviate some shortfalls in the health sector, where the transfer of records from one system to another is not on par with other sectors.

Is R&D Needed? Yes, for sectors such as healthcare (portability of medical records from province to province) and the creation of a categorial structure for data elements.

Recommendation: To standardize the preservation of information exchange between systems so that data can be exported in a digital format by data controllers with its detailed structure, metadata and links to other data. Also, to identify the circumstances under which data about data subjects can be removed by a data controller and the implications that this has on other related data (e.g., the right to be forgotten).

Priority: Medium/Low.

Organization(s): ISO/IEC

Working Group 4: Data Analytics, Solutions and Commercialization

Issue 30 — Technical Elements of AI Solutions

This issue covers the technical elements of AI solutions referring to technologies, software, and platforms. This includes the terminology used (including artificial intelligence itself), the subcategories of artificial intelligence, describing the lifecycle and individual components. Included in scope is the analysis, verification and validation in selection and use of AI solutions and platforms.

With the rapidly evolving innovations in AI technologies, having a common language would help to ease regulators, innovators and consumers in their conversations. There are many published and proposed definitions, but there is a lack of consensus and a poor understanding of the adoption of these terms. Furthermore, more work is needed to describe the AI lifecycle and to focus on the framework of quality assurance, not just from a policy perspective but from a technical analysis of verification and validation.

This area has high interest and activity across the regulatory, industry and standards landscape. There is emerging work done in ISO/IEC JTC 1/SC 42 on the AI lifecycle, as well as work on how best to validate components of the lifecycle. A sector-specific approach is also underway, with work beginning in the health sector, looking at software as a medical device approach towards AI. This is an area where work is just beginning. There are many opportunities still emerging and coordination is needed for a consistent Canadian approach.

Gap: Technical Elements of AI Solutions. The scope of this issue generated a large number of standards, most of them not relevant, and a number that are indirectly relevant or sector specific. The sector-specific standards were mainly health and transportation applications of AI systems. A missing stakeholder group was the public service and standards that could be used by it. The limited number of standards directly targeting the issue indicates the beginning of standards development in this area, with several under development. Further supporting this indication, more than one-third of the standards examined for this issue were developed in 2015 or later.

Is R&D Needed? Yes

Recommendation: To standardize a terminology and the lifecycle components to lay the groundwork for the interoperability of AI solutions, and specifications for verification and validation.

Priority: High/Medium

Organization(s): AI industry associations, diverse regulatory bodies across jurisdictions and at the federal level, international SDO

Issue 31 — Data Value Chain

This issue covers monetization (as a framework for creating new value chains for data assets) and the role of intellectual property in data.

This is an area that requires more description and identification. Most efforts currently focus on the description of the data lifecycle. While there is consensus that the valuation of data is of high importance, particularly in transaction of data exchange, there is little to no guidance for valuation, or any frameworks for creating new value chains for data assets. There is a need for more structure in how monetization is described, as well as methodologies for efficient transactions that are fair to both parties.

Gap: Data Value Chain. There are not many standards generated for this issue. There was a select representation of different sectors, particularly transportation and health. There were a few standards that were related in particular to the data value and collection in smart cities. There was a lack of standards from the financial sector. There was a significant amount of standards that pertained to data portability and storage in the blockchain application, however none within that were within the scope of artificial intelligence. The keywords listed in this issue search did generate standards pertaining to data governance at large. It is interesting to note that more than one-third of the standards examined for this issue were developed in 2015 or after, which indicates strong standardization activities aiming to address this issue.

Is R&D Needed? Yes

Recommendation: To standardize the system by which valuation is applied to data and its implications on data exchanges and transactions.

Priority: Medium/Low

Organization(s): National, regional or international SDO

Issue 32 — Transparency and Communication of Data Analytics

This issue covers disclosure and communication of data analytics, as well as disclosure of exposure to risks for data owners. The perspective of this issue is from the lens of the data supply chain. The term “disclosure” can have a legal connotation, and thus the issue title includes the term “transparency.” This will include how risks and processes are communicated, and the transparency which is included for users as well as data owners.

There are concerns over the level of disclosure and the communication of the level of data analytics that are conducted to the data owners and consumers at large. These concerns are as yet unsolved and, while individual cases are raised by the media as well as regulator concerns, there is a lack of coordinated options for adequate disclosure. Whenever one parts with information, the risks of personal identification and possible future risk are not immediately clear or disclosed. There is a lack of awareness and a lack of structure in how to communicate the different levels of risk. Another aspect to consider with this issue is the audience for the scope. The level of transparency and communication may differ based on who is receiving the information, whether it be the suppliers, regulators, third parties or clients.

A current example of this issue is the data collection in the midst of the COVID-19 pandemic. There is a marked concentration of health data collection and considerations for location tracking, creating a risk score. Furthermore, there have been options to create a nutrition label for data, which would increase the explainability. This would help to increase the awareness about the metadata created, frameworks used and standardized lexicon. Another possible concept is the development of data sheets for data sets. There are requests for structured levels of the type of disclosure that is required based on sensitivities. Personal data gives another layer of concern, both for the owners of the data, as well as analytics that use it. There have been regulatory initiatives in this space, the most well-known being the work in the EU Commission, the General Data Protection Regulation (GDPR). Examples of this issue have been raised in both the financial and energy sector. The level of transparency in financial transactions has been important in detecting money laundering and fraud, but also raises concern over the level of privacy that citizens have. The Ontario Energy Board has addressed the level of transparency with regard to energy usage through its online communications and regulations. As a municipal example, the Sidewalk Labs project in Toronto, while now closed, developed an iconography to identify what type of data is collected.

As a part of working group discussions, terms were scoped in the following ways:

(data) Ownership:

- Public/individual ownership of personal data
  - Shared purposefully (e.g., DNA tests, credit/point card purchases)
  - Shared unknowingly (e.g., CCTV, facial recognition)
  - Personal data in public domain
- Corporate ownership of collected data
- Government ownership of collected data
- Academic ownership of collected data

(data) Collector:

- Original data capture
- Users of existing data collections
- Anonymizes/disaggregates data (e.g., covid app)

(data) Custodian:

- Maintaining data quality, storage and accessibility
- Maintaining list of users and to whom data has been shared for ongoing tracking/monitoring
- Training users to recognize unconscious/implicit bias
- Developing/delivering bias training adapted to type of user (operational versus policy versus strategic versus technical)
- Defining approaches to address different types of data problems (operational versus policy versus strategic versus technical); very diverse, ensuring no one-size-fits-all solution
- Maintain ability for individual owner to remove their data/consent of use of their data (e.g., Google, Twitter archive at Library of Congress)

- Maintaining disaggregation/anonymity in data
- Monitoring system interactions and decision making

(data) User:

- Corporate versus government versus academic versus independent versus individual
- Impact of academic research rights regarding personal information

(data) Governance:

- Monitor/correct system or user scope/scope creep (i.e., the problem and data used for the solution to the problem should align)
- Setting/updating guidelines for managing system-to-system information sharing (where there is no human interaction)
- Setting monetary consequences for breaches/bias
- Determining/setting the value of data collected
- Determining risk probability/classification/mapping/appetite/thresholds/mitigation for data and systems
- Internal/industry governance, best practices and government regulations/legislation

Gap: Transparency and Communication of Data Analytics. Based on the description of the joint issues, there is a possibility that standards results from issues in other working groups could be useful for stakeholders looking at these issues. There were many results in the search for these issues. One of the main observations of the results was that the keywords that appeared in these standards are not used in the same way as they were defined in the issue description. As a result, many standards found were not applicable. There were several standards that were found in Tier II that would be useful in leveraging when exploring opportunities for standards for Tier I. There were also a number of sector-specific standards which could be applicable, although their scope was narrow.

Is R&D Needed? Yes

Recommendation: To standardize the process and terminology by which data owners are informed of what happens to their data and what possible risks sharing their data may incur.

Priority: High.

Organization(s): AI industry associations, diverse regulatory bodies across jurisdictions and at the federal level, international SDO

Issue 33 —
Interpretability and Explainability of AI Systems

(Originally "Interpretability of Algorithms")

This issue covers transparency of the capabilities and functions of an algorithm. In the depth and pace of innovation, there is a need for a minimum level of requirements to ascertain interpretability of the solutions and products created through advanced data analytics. This will enable the stability of the development of future applications across different sectors.

There is a focus on the lack of explainability with algorithms. There is an apparent conflict in the need for transparency, while acknowledging that the innovation is the ability to adapt and change during the course of analytics. This poses further challenges when looking at a complex system where there may be levels of algorithms providing decision-making recommendations. In sectors where a high level of regulation exists, this poses further challenges in how to communicate assurance to regulators that existing frameworks are being followed.

Gap: Interpretability and Explainability of AI systems. The keywords selected in this issue generated many results, however none of them could be classified as Tier I. The majority of the results used the keywords in a different context than described in this issue. There were standards found that fit into Tier II, addressing areas that supported the issue from a perspective of risk management in information technology. There is a need for standards in this area to address the identified needs of stakeholders, both in sector-specific standards and general broad application.

Is R&D Needed? Yes

Recommendation: To standardize the way that AI system capabilities and results are explained in human terms.

Priority: Medium

Organization(s): National, regional or international SDO

Issue 34 —
Assessment and Management of Bias

Bias has been identified as a key issue in how it is identified and, if necessary, managed. Bias has been defined as the systematic difference in treatment in any kind of action, including perception, observation, representation, prediction or decisions of certain objects, people or groups in comparison to others. This particular issue is linked with the issue of performance management but has been created as a standalone issue to focus on the complexities as well as sensitivities of bias.

Algorithms and data analytics are poised to provide solutions and recommendations which will have an impact on our everyday life. As such, a high level of scrutiny is needed in how those solutions and recommendations are achieved and what factors are influencing the outcomes. When those solutions and recommendations impact the day-to-day life of society, it is important to see if any preconceived notions have entered the process. Some technologies are purposefully built with certain bias. There is a need to address how to take this into consideration when using technologies built with certain bias. The possible risks can have very high consequences and, as such, it is important to study it as a standalone issue.

There have been many media cases pointing out the pitfalls when bias is included in AI systems. There have been news articles of racist recommendations from AI systems on recidivism rates in the United States being skewed due to years of biased policing. People have expressed concern about whether any medical or financial decisions would be made based on outcomes that have discriminatory angles, or an incomplete data set on the needed demographic. Bias may very well come into play if decisions are based on irrelevant attributes such as appearance (e.g., higher insurance premiums for youth), but is it bias if decisions are made purely based on data supporting the fact, such as that a youth is more likely to get into an accident than a non-youth? Recently, the possible biased consequences of facial recognition has been highlighted by media.

The issue identified has been the result of wider adoption of technologies and innovation. Work continues to be underway and as further adoption continues, further questions as well as solutions will emerge. It is important to make clear that it is inaccurate and in itself a form of implicit bias to assume and declare that there is no bias in a dataset or system without validated, expert proof.

Out of Scope: Bias as outlined in WG 1 & WG 2.

Gap: Assessment and Management of Bias. The keywords selected in this issue generated a succinct batch of results, however none of them could be classified as Tier I. The majority of results used the keywords in a different context than described in this issue. There was a particular standard found that fit into Tier II, addressing the area of trustworthiness, which includes the sections described above around bias. There is a need for standards in this area to address the identified needs of stakeholders, both in sector-specific standards as well as general broad application.

Is R&D Needed? Yes

Recommendation: To standardize the types of protocols, processes and assessments used in identifying bias, as well as standardizing the management of bias where necessary.

Priority: Medium

Organization(s): National, regional or international SDO

Issue 35 —
Performance Management Systems for Analytics and AI Systems

The focus of this issue is internal governance, from the analysis of risk level to the design and deployment of models, algorithms and systems. This issue is scoped to look at the high level of performance management, with a view to how any interactions with humans may be managed. Included in the scope is the discussion of the use of management system standards in the space of artificial intelligence, a lack of trust as well as guidance in deploying and using AI systems, algorithms, data analytics models within existing organizations, as well as how consumers and end-users assess the frameworks in place.

Along with the development of industry in this sector, there is a need for a risk-based governance of AI, where organizations can address performance management based on their "risk profile." The need for this has been shown in the standards under development, such as ISO/IEC 38507 – Information technology- Governance of IT- Governance. Furthermore, there is a growing movement around developing a standard that specifies the requirements and provides guidance for establishing, implementing, maintaining and continually improving an artificial intelligence management system within the context of an organization. This addresses the sector-agnostic need for governance in performance management, as well as sets the foundation for future sector-specific needs.

Gap: Performance Management Systems for Analytics and AI Systems. The search resulted in a number of standards. The majority were not applicable to the keywords or the issue as described. The rest of the search results were standards that were either general management and/or governance standards, or standards that applied to traditional sectors. There were standards that, while they cannot be applied to the issue, would serve as good reference in the development of Tier I standards. It should be noted that at time of publication of this Roadmap, ISO/IEC are in the preparatory stages of ISO/IEC 42001 Artificial Intelligence Management System Standard, which will contain AI specific process requirements that would allow for assessment or conformance of auditability of the processes.

Is R&D Needed? Yes

Recommendation: To standardize the governance approaches in organizations that use or create AI systems, encouraging diverse participation in the development of conformity assessment-based standards such as ISO/IEC 42001 Artificial Intelligence Management System Standard.

Priority: Medium

Organization(s): AI industry associations, diverse regulatory bodies across jurisdictions and at the federal level, international SDO

Annex B —

List of Tier 1 Published Standards and Related Materials for Key Issues

Working Group 1: Foundations of Data Governance

Issue 1 — Accountability Framework

IEEE STDVA24228	Big Data Governance and Metadata Management: Standards Roadmap
ISO/TR 24514	Activities relating to drinking water and wastewater services – Examples of the use of performance indicators using ISO 24510, ISO 24511 and ISO 24512 and related methodologies
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
SAE GEIA-HB-859	Implementation Guide for Data Management – Formerly TechAmerica GEIA-HB-859
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ITU-T H.860	Multimedia e-health data exchange services: Data schema and supporting services – Study Group 16
ITU-T Y.3514	Cloud computing – Trusted inter-cloud computing framework and requirements – Study Group 13
CEN/TR 17370	Public transport – Operating raw data and statistics exchange
ISO 11240	Health informatics – Identification of medicinal products – Data elements and structures for the unique identification and exchange of units of measurement
ISO 15394	Packaging – Bar code and two-dimensional symbols for shipping, transport and receiving labels
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiable information protection
ISO/IEC 29187-1	Information technology – Identification of privacy protection requirements pertaining to learning, education and training (LET) – Part 1: Framework and reference model
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

ISO/IEC 29184:2020	Information technology – Online privacy notices and consent
ISO/IEC WD TS 27560	Privacy technologies – Consent record information structure
n/a	A Guide for Ethical Data Science
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
IEEE P7002	Data Privacy Process
IEEE P7004	Standard for Child and Student Data Governance
IEEE P7005	IEEE Draft Standard for Transparent Employer Data Governance
IEEE P2089	Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children
IEEE P3800	Standard for a data-trading system: overview, terminology and reference model
IEEE P2895	Standard Taxonomy for Responsible Trading of Human-Generated Data
IC16-002	The Global Initiative on Ethics of Autonomous and Intelligent Systems
IC19-004	Technology and Data Harmonization for Enabling Clinical Decentralized Clinical Trials
IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

Issue 2 — Certification for Professional Roles

ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

COBIT 2019	Effective IT Governance at Your Fingertips – Build your expertise in the globally accepted framework for optimizing enterprise IT governance.
n/a	ISACA CREDENTIALS
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CIOSC 102	Qualification and certification of big data and machine learning personnel
CAN/CIOSC 109-1	Qualification and proficiency of privacy and access control professionals
ISO/IEC/IEEE 24765:2017	International Standard – Systems and software engineering – Vocabulary

Issue 3 — Digital Literacy

ITU-T L.1505	Information and communication technology and adaptation of the fisheries sector to the effects of climate change – Study Group 5
ISO 21248	Information and documentation – Quality assessment for national libraries – First edition
ISO/IEC TR 18120	Information technology – Learning, education, and training – Requirements for e-textbooks in education – First Edition

ISO/IEC 18120	Information technology – Learning, education, and training – Requirements for e-textbooks in education
ISO/IEC 19788-5	Information technology – Learning, education and training – Metadata for learning resources Part 5: Educational elements
ISO/IEC TR 18120	Information technology – Learning, education, and training – Requirements for e-textbooks in education
BSI PAS 1040	Digital readiness – Adopting digital technologies in manufacturing – Guide
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap Part 2: Architectural components and maturity model
DS DS/CWA 16213	End User e-Skills Framework Requirements
DS DS/CWA 16266	Curriculum for training ICT Professionals in Universal Design

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

n/a	Levelling Up: The Quest for Digital Literacy
n/a	Improving Canada's Digital Advantage: Building the Digital Talent Pool and Skills for Tomorrow
n/a	TELUS Wise
n/a	What is digital literacy?
n/a	Digital Literacy Framework Yukon Education
n/a	Elements of AI free online course
n/a	Certified Ethical Emerging Technologies
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
IEEE 3527.1-2020	IEEE Approved Draft Standard for Digital Intelligence (DQ) – Framework for Digital Literacy, Skills and Readiness
IEEE P2089	Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children
IEEE P7011	Standard for the Process of Identifying and Rating the Trustworthiness of News Sources

Issue 4 — Cybersecurity Protection

ISO/IEC 29100	Information technology – Security techniques – Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)
ISO/IEC TR 27103	Information technology – Security techniques – Cybersecurity and ISO and IEC Standards
CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
CENELEC EN 50584	Information technology – CENELEC/ETSI Glossary of terms and definitions for broadband deployment including sustainability aspects
CENELEC EN 50173-1	Information technology – Generic cabling systems Part 1: General requirements
CENELEC EN 50173-2	Information technology – Generic cabling systems – Part 2: Office spaces
CENELEC EN 50173-5	Information technology – Generic cabling systems Part 5: Data centre spaces
ISO/IEC 8348	Information technology – Open Systems Interconnection – Network dervice definition
ISO/IEC 17788	Information technology – Cloud computing – Overview and vocabulary
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture

ITU-T Y.3500	Information technology – Cloud computing – Overview and vocabulary – Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ISO/IEC 15504.5	Information technology – Process assessment Part 5: An exemplar software life cycle process assessment model
ISO/IEC 15504-5	Information technology – Process assessment Part 5: An exemplar software life cycle process assessment model
ISO/IEC 18028.2	Information technologySecurity techniquesIT network security Part 2: Network security architecture – ISO/IEC 18028-2:2006
ISO/IEC 19770-8	Information technology – IT asset management Part 8: Guidelines for mapping of industry practices to/ from the ISO/IEC 19770 family of standards
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
ISO/IEC 27034-5	Information technology – Security techniques – Application security Part 5: Protocols and application security controls data structure
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29115	Information technology – Security techniques – Entity authentication assurance framework
ISO/IEC 29190	Information technology – Security techniques – Privacy capability assessment model
ISO/IEC 30100-2	Information technology – Home network resource management – Part 2: Architecture
ISO/IEC 30105-2	Information technology – IT Enabled Services-Business Process Outsourcing (ITES-BPO) lifecycle processes Part 2: Process assessment model (PAM)
ISO/IEC 38500	Information technology – Governance of IT for the organization
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data
ISO/IEC 38506	Information technology – Governance of IT – Application of ISO/IEC 38500 to the governance of IT enabled investments
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TS 27034-5-1	Information technology – Application security Part 5-1: Protocols and application security controls data structure, XML schemas
SNZ AS/NZS 15271	Guide for AS/NZS ISO/IEC 12207 (Information Technology) – Software Life Cycle Processes)
CEN EN 16571	Information technology – RFID privacy impact assessment process
ISO/IEC/IEEE 42030	Software, systems and enterprise – Architecture evaluation framework
CENELEC EN 50667	Information technology – Automated infrastructure management (AIM) systems – Requirements, data exchange and applications
ISO/IEC 18028-5	Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks
ISO/IEC 18043	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems
ISO/IEC 20243-2	Information technology – Open Trusted Technology ProviderTM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products Part 2: Assessment procedures for the O-TTPS and ISO/ IEC 20243-1:2018
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation of virtualized servers
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management – Part 3: Practice

ISO/IEC 27034-1	Information technology – Security techniques – Application security Part 1: Overview and concepts – CORR: February 28, 2014
ISO/IEC 27034-2	Information technology – Security techniques – Application security Part 2: Organization normative framework
ISO/IEC 27034-3	Information technology – Application security Part 3: Application security management process
ISO/IEC 27039	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS) – CORR: June 30, 2018
ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment – CORR: April 30, 2020
ISO/IEC TR 13335-5	Information Technology – Guidelines for the Management of IT Security – Part 5: Management Guidance on Network Security (TECHNICAL REPORT)
ISO/IEC TR 14516	Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services (Technical Report)
ISO/IEC TR 15443-1	Information technology – Security techniques – Framework for IT security assurance – Part 1: Overview and Framework (Technical Report)
ISO/IEC TR 15443-2	Information technology – Security techniques – Security assurance framework – Part 2: Analysis (Technical Report)
ISO/IEC TR 15443-3	Information technology – Security techniques – A framework for IT security assurance – Part 3: Analysis of assurance methods
ISO/IEC TR 19791	Information technology – Security techniques – Security assessment of operational systems (Technical Report)
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 29156	Information technology – Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
ISO/IEC TR 29181-5	Information technology – Future Network – Problem statement and requirements Part 5: Security
ITU-T STIT	Security in Telecommunications and Information Technology – Study Group 17
ITU-T X.842	Information technology – Security techniques – Guidelines for the use and management of trusted third party services – Study Group 7
ISO/IEC 27006	Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
DIN SPEC 91367	Urban mobility data collection for real-time applications; Text in English
ISO 14641	Electronic document management – Design and operation of an information system for the preservation of electronic documents – Specifications
ISO 29134	Information technology – Security techniques – Guidelines for privacy impact assessment (ISO/IEC 29134:2017)
ISO/IEC 10021-8	Information technology – Message Handling Systems (MHS) – Part 8: Electronic Data Interchange Messaging Service
ISO/IEC 18045	Information technology – Security techniques – Methodology for IT security evaluation
ISO/IEC 20944-1	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) Part 1: Framework, common vocabulary, and common provisions for conformance
ISO/IEC 23736-3	Information technology – Digital publishing – EPUB 3.0.1 Part 3: Content documents
ISO/IEC 27034-6	Information technology – Security techniques – Application security – Part 6: Case studies
ISO/IEC 27034-7	Information technology – Application security Part 7: Assurance prediction framework
ISO/IEC 29147	Information technology – Security techniques – Vulnerability disclosure
ISO/IEC 30111	Information technology – Security techniques – Vulnerability handling processes
ISO/IEC TS 19249	Information technology – Security techniques – Catalogue of architectural and design principles for secure products, systems and applications

ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operational environment
ISO/IEC TS 22237-6	Information technology – Data centre facilities and infrastructures Part 6: Security systems
ISO/IEC 27033-5	Information technology – Security techniques – Network security Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

n/a	National Cyber Security Strategy
ISO 20252:2019	Market, opinion and social research, including insights and data analytics – Vocabulary and service requirements
ISO 19092:2008	Financial services – Biometrics – Security framework
ISO/TR 22100-4:2018	Safety of machinery – Relationship with ISO 12100 – Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CIOSC/PAS 100-4:2020	Data governance – Part 4: Specification for Scalable Remote Access Infrastructure
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
CAN/CIOSC 103-3	Digital trust and identity – Part 3: Digital credentials
CAN/CIOSC 103-4	Digital trust and identity – Part 4: Digital wallets
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
CAN/CIOSC 105	Cybersecurity of Industrial Internet of Things (IIoT) devices and systems
IEEE P2658	Guide for Cybersecurity Testing in Electric Power Systems
IEEE P1547.3	Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
IEEE P2808	Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems
IEEE P9274.4.2	Recommended Practice for Cybersecurity in the Implementation of the Experience Application Programming Interface (xAPI)
IEEE P2418.9	Standard for Cryptocurrency Based Security Tokens
IEEE P2933	Standard for Clinical Internet of Things (IoT) Data and Device Interoperability with TIPPSS – Trust, Identity, Privacy, Protection, Safety, Security
IEEE P1609.2	Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages
IEEE P802.15.4y	IEEE Draft Standard for Low-Rate Wireless Networks Amendment Defining Support for Advanced Encryption Standard (AES)-256 Encryption and Security Extensions
IEEE P802.1AEdk	Standard for Local and metropolitan area networks-Media Access Control (MAC) Security Amendment 4: MAC Privacy protection
IEEE P1912	Standard for Privacy and Security Framework for Consumer Wireless Devices
IEEE P2621 series	Wireless Diabetes Device Security Assurance (3 projects under development)
IEEE P1711.1	Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links: Substation Serial Protection Protocol
IEEE P1686	Standard for Intelligent Electronic Devices Cyber Security Capabilities

IEEE 2030.102.1-2020	IEEE Approved Draft Standard for Interoperability of Internet Protocol Security (IPsec) Utilized within Utility Control Systems
ISO/IEC 27400	Cybersecurity – IoT security and privacy – Guidelines
ISO/IEC 27402	Cybersecurity – IoT security and privacy – Device baseline requirements
ISO/IEC 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
CSA T100**	ICT Code for Buildings
CSA T200**	Evaluation of software development and cybersecurity programs (update to CSA EXP 200)
CSA EXP 200	Evaluation of software development and cybersecurity programs
CSA T2000-1**	Intelligent Building System Objective Code
CSA T2000-2**	Intelligent Building System Safety Management System Code
CSA Z246.1	Security management for petroleum and natural gas industry systems
CSA N290.7	Cyber security for nuclear power plants and small reactor facilities
CSA T150**	Connected and automated vehicle code
CSA T710**	Smart manufacturing readiness assessment methodology and requirements
CAN/CSA-ISO 14971	Medical Devices – Application of Risk Management to Medical Devices
CAN/CSA-CEI/IEC 62304	Medical device software – Software life cycle processes

Issue 5 — Data Management Governance

ISO/IEC TR 38505-2:19	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO 19731	Digital analytics and web analyses for purposes of market, opinion and social research – Vocabulary and service requirements – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

ISO 28500:2017	Information and documentation – WARC file format
ISO/IEC 38500:2015	Information technology – Governance of IT for the organization
ISO/IEC 38505-1:2017	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
n/a	DCAM: The Data Management Capability Assessment Model
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
ISO/IEC/IEEE 42020:2019(E)	ISO/IEC/IEEE International Standard – Software, systems and enterprise – Architecture processes
ISO/IEC/IEEE 24765:2017	ISO/IEC/IEEE International Standard – Systems and software engineering – Vocabulary
CSA T100**	ICT Code for Buildings
CSA T200**	Evaluation of software development and cybersecurity programs (update to CSA EXP 200)
CSA EXP 200	Evaluation of software development and cybersecurity programs
CSA T2000-1**	Intelligent Building System Objective Code

CSA T2000-2**	Intelligent Building System Safety Management System Code
CSA Z246.1	Security management for petroleum and natural gas industry systems
CSA N290.7	Cyber security for nuclear power plants and small reactor facilities
CSA T150**	Connected and automated vehicle code
CSA T710**	Smart manufacturing readiness assessment methodology and requirements
Z1635**	Canadian Paramedic Information System
CSA Z8000	Canadian health care facilities

Issue 6 — Data Privacy (consolidated with Issue: Data rights)

ANSI X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography
ANSI X9.63	Public Key Cryptography for the Financial Services Industry Key Agreement and Key Transport Using Elliptic Curve Cryptography
ANSI X9.73	Cryptographic Message Syntax – ASN.1 and XML – ASCX9
ANSI X9.84	Biometric Information Management and Security for the Financial Services Industry
ANSI INCITS 446	Information Technology – Identifying Attributes for Named Physical and Cultural Geographic Features (Except Roads and Highways) of the United States, Territories, Outlying Areas, and Freely Associated Areas, and the Waters of the Same to the Limit of the Twelve-Mile Statutory Zone
ASA S12.70	American National Standard Criteria for Evaluating Speech Privacy in Healthcare Facilities
ASCE GSP 226	Geotechnical Engineering State of the Art and Practice Keynote Lectures from GeoCongress 2012
ASTM E2369	Standard Specification for Continuity of Care Record (CCR)
ASTM E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
ASTM E2468	Standard Practice for Metadata to Support Archived Data Management Systems
ASTM E2259 REV A	Standard Guide for Archiving and Retrieving Intelligent Transportation Systems-Generated Data
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
CEN EN 14302	Health informatics – Framework for security requirements for intermittently connected devices
CEN EN 12924	Medical informatics – Security Categorisation and Protection for Healthcare Information Systems
CEN EN 13608-3	Health informatics – Security for healthcare communication – Part 3: Secure data channels
CEN/TR 16742	Intelligent transport systems – Privacy aspects in ITS standards and systems in Europe
CEN EN 15969-1	Tanks for transport of dangerous goods – Digital interface for the data transfer between tank vehicle and with stationary facilities – Part 1: Protocol specification – Control, measurement and event data
CEN EN 15969-2	Tanks for transport of dangerous goods – Digital interface for the data transfer between tank vehicle and with stationary facilities – Part 2: Commercial and logistic data
CEN EN 13032-1	Light and lighting – Measurement and presentation of photometric data of lamps and luminaires – Part 1: Measurement and file format – Incorporates Amendment A1: 2012
CEN/TS 15430-2	Winter and road service area maintenance equipment – Data acquisition and transmission – Part 2: Protocol for data transfer between information supplier and client application server
CEN EN 13757-7	Communication systems for meters – Part 7: Transport and security services
CENELEC EN 50491-11	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Part 11: Smart Metering – Application Specifications – Simple External Consumer Display
CGSB CAN/CGSB-133.1-2017	Security officers and security officer supervisors
CAN/CIOSC 109-1	Qualification and proficiency of privacy and access control professionals

CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
CLSI M39-A4	Analysis and Presentation of Cumulative Antimicrobial Susceptibility Test Data; Approved Guideline – Fourth Edition; Vol. 34; No. 2
CLSI AUTO10-A	Autoverification of Clinical Laboratory Test Results; Approved Guideline – First Edition; Vol 26; No 32
CLSI MM20-A	Quality Management for Molecular Genetic Testing; Approved Guideline – Vol 32; No 15
CSA Q830	Model Code for the Protection of Personal Information
CSA B480-02	Customer Service Standard for People with Disabilities – First Edition
CSA B480-02 LARGE PRINT	Customer Service Standard for People with Disabilities – First Edition
CSA CAN/ CSA-B651.2-07	Accessible design for self-service interactive devices – First Edition
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ETSI TR 102 612	Human Factors (HF); European accessibility requirements for public procurement of products and services in the ICT domain (European Commission Mandate M 376, Phase 1) – V1.1.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TR 101 584	Machine-to-Machine Communications (M2M); Study on Semantic support for M2M Data
ETSI EN 300 392-1 V1.6.1	Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI GS INS 002	Identity and Access Management for Networks and Services Distributed Access Control for Telecommunications Use Cases and Requirements – V1.1.1
ETSI TR 102 764	eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 133 501	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.4.0 Release 16)
IEC 62443-4-2	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components
IEC 61158-4-2	Industrial communication networks – Fieldbus specifications – Part 4-2: Data-link layer protocol specification – Type 2 elements
IEC 61158-4-25	Industrial communication networks – Fieldbus specifications – Part 4-25: Data-link layer protocol specification – Type 25 elements
IEC TS 63134	Active assisted living (AAL) use cases
IEEE 1888 SERIES	Ubiquitous Green Community Control Network Protocol – Includes IEEE 1888; IEEE 1888.1; IEEE 1888.2; IEEE 1888.3; IEEE 1888.4
IEEE 802.1AE	Local and Metropolitan Area Networks – Media Access Control (MAC) Security – IEEE Computer Society
IEEE 2410	Biometric Open Protocol
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 802.17	Information technology—Telecommunications and information exchange between systems Local and metropolitan area networks—Specific requirements Part 17: Resilient packet ring (RPR) access method and physical layer specifications – IEEE Computer Society

IES LM-63	APPROVED METHOD: IES STANDARD FILE FORMAT FOR THE ELECTRONIC TRANSFER OF PHOTOMETRIC DATA AND RELATED INFORMATION
ISO 11577	Information technology – Open Systems Interconnection – Network layer security protocol
ISO 18185-4	Freight containers – Electronic seals – Part 4: Data protection
ISO 20215	Space data and information transfer systems – CCSDS cryptographic algorithms – First Edition
ISO 21091	Health informatics – Directory services for healthcare providers, subjects of care and other entities
ISO 21324	Space data and information transfer systems – Space data link security protocol – First Edition
ISO 21549-2	Health informatics – Patient healthcard data – Part 2: Common objects (ISO 21549-2:2014); English version EN ISO 21549-2:2014
ISO 21549-3	Health informatics – Patient healthcard data – Part 3: Limited clinical data (ISO 21549-3:2014); English version EN ISO 21549-3:2014
ISO 21549-4	Health informatics – Patient healthcard data – Part 4: Extended clinical data (ISO 21549-4:2014); English version EN ISO 21549-4:2014
ISO 21549-5	Health informatics – Patient healthcard data – Part 5: Identification data
ISO 21549-6	Health informatics – Patient healthcard data – Part 6: Administrative data
ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799:2016)
ISO/IEC 10116	Information technology – Security techniques – Modes of operation for an n-bit block cipher
ISO/IEC 10181-5-00	Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework
ISO/IEC 11577-97	Information technology – Open Systems Interconnection – Network layer security protocol
ISO/IEC 19772	Information technology – Security techniques – Authenticated encryption
ISO/IEC 19794-11	Information technology – Biometric data interchange formats – Part 11: Signature/sign processed dynamic data
ISO/IEC 19794-13	Information technology – Biometric data interchange formats – Part 13: Voice data
ISO/IEC 19794-7	Information technology – Biometric data interchange formats – Part 7: Signature/sign time series data
ISO/IEC 24713-2	Information technology – Biometric profiles for interoperability and data interchange – Part 2: Physical access control for employees at airports
ISO/IEC 29150/	Information technology – Security techniques – Signcryption
ISO/IEC 30107-2	Information technology – Biometric presentation attack detection – Part 2: Data formats
ISO/IEC/IEEE 18883	Information technology – Ubiquitous green community control network – Security
ISO 10781	Health Informatics – HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM) – Second Edition
ISO TS 27790	Health informatics – Document registry framework – First Edition
ISO 20078-3	Road vehicles – Extended vehicle (ExVe) web services – Part 3: Security
ISO TR 12859	Intelligent transport systems – System architecture – Privacy aspects in ITS standards and systems – First Edition
ISO 12855	Electronic fee collection – Information exchange between service provision and toll charging
ISO 13399-1	Cutting tool data representation and exchange – Part 1: Overview, fundamental principles and general information model
ISO 18440	Space data and information transfer systems – Space link extension – Internet protocol for transfer service – Second Edition
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO 20208	Space data and information transfer systems – Delta-DOR Raw Data Exchange Format – First Edition
ISO 21076	Space data and information transfer systems – Space communications cross support – Architecture requirements document – First Edition

ISO 22663	Space data and information transfer systems – Proximity-1 space link protocol – Data link layer – Third Edition
ISO/IEC 17417	Information technology – Telecommunications and information exchange between systems – Short Distance Visible Light Communication (SDVLC) – First Edition
ISO/IEC 20248	Information technology – Automatic identification and data capture techniques – Data structures – Digital signature meta structure – First Edition
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ISO TS 22220	Health informatics – Identification of subjects of health care – Second Edition
ISO/IEC 13871-97	Information technology – Telecommunications and information exchange between systems – Private telecommunications networks – Digital channel aggregation
ISO/IEC 9798-6	Information technology – Security techniques – Entity authentication – Part 6: Mechanisms using manual data transfer
ISO/TS 22220	Health informatics – Identification of subjects of health care
ISO/IEC/IEEE 8802-3	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 3: Standard for Ethernet
ISO 15396	Space data and information transfer systems – Cross support reference model – Space link extension services
ISO 18750	Intelligent transport systems – Co-operative ITS – Local dynamic map (ISO 18750:2018)
ISO 23354	Business requirements for end-to-end visibility of logistics flow – First edition
ISO/IEC 24761:20	Information technology – Security techniques – Authentication context for biometrics
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing
ISO/TR 23786	Road vehicles – Solutions for remote access to vehicle – Criteria for risk assessment
ISO/TR 23791	Road vehicles – Extended vehicle (ExVe) web services – Result of the risk assessment on ISO 20078 series
ISO/TS 18750	Intelligent transport systems – Cooperative systems – Definition of a global concept for Local Dynamic Maps (ISO/TS 18750:2015); English version CEN ISO/TS 18750:2015
ISO/IEC 27034-6	Information technology – Security techniques – Application security – Part 6: Case studies
ISO 22857	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health data – Second Edition
ISO/IEC 15944-12	Information technology – Business operational view – Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI) – First edition
ISO TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – First Edition
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – CORR: February 28, 2014
ISO TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information – First Edition
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ITU-T G.9961	Unified high-speed wireline-based home networking transceivers – Data link layer specification – Study Group 15
ITU-T Y.4468	Minimum set of data transfer protocol for automotive emergency response system – Study Group 20

ITU-T Q.1229	Intelligent Network User's Guide for Capability Set 2 – Series Q: Switching and Signalling – Intelligent Network – Study Group 11; 175pp
ITU-T Y.3509	Cloud computing – Functional architecture for data storage federation – Study Group 13
ITU-T SERIES Q SUPP 30	Supplement to ITU-T Recommendation Q.1701 – Roadmap to IMT-2000 Recommendations, Standards and Technical Specifications – Study Group 11
ITU-T SERIES Y SUPP 30	ITU-T Y.4250 series – Smart sustainable cities – Overview of smart sustainable cities infrastructure – Study Group 20
ITU-T X.1642	Guidelines for the operational security of cloud computing – Study Group 17
ITU-T Y.1311.1	Network-Based IP VPN Over MPLS Architecture Series Y: Global Information Infrastructure and Internet Protocol Aspects Internet Protocol Aspects – Transport – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
SAE AIR6904	Rationale, Considerations, and Framework for Data Interoperability for Health Management within the Aerospace Ecosystem
SAE ARP4294	Data Formats and Practices for Life Cycle Cost Information
SAE GEIA-HB-0007-B	(R) Logistics Product Data Handbook – Formerly TechAmerica SAE GEIA-HB-0007-B
UL 2196	UL Standard for Safety Fire Test for Circuit Integrity of Fire-Resistive Power, Instrumentation, Control and Data Cables – Second Edition; Reprint with revisions through and including November 30, 2018

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

IEEE P7002	Data Privacy
DIACC PCTF 04	Pan-Canadian Trust Framework (PCTF) Privacy: Component Overview and Conformance Profile v1.0
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent: Component Overview and Conformance Profile v1.0
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
CAN/CIOSC 109-1	Qualification and proficiency of privacy and access control professionals
ISO/IEC 27400	Cybersecurity – IoT security and privacy – Guidelines
ISO/IEC 27402	Cybersecurity – IoT security and privacy – Device baseline requirements
ISO/IEC 27403	Cybersecurity – IoT security and privacy – Guidelines for IoT-domotics
CSA T100**	ICT Code for Buildings
CSA T200**	Evaluation of software development and cybersecurity programs (update to CSA EXP 200)
CSA EXP 200	Evaluation of software development and cybersecurity programs
CSA T2000-1**	Intelligent Building System Objective Code
CSA T2000-2**	Intelligent Building System Safety Management System Code
CSA Z246.1	Security management for petroleum and natural gas industry systems
CSA N290.7	Cyber security for nuclear power plants and small reactor facilities
CSA T150**	Connected and automated vehicle code

CSA T710**	Smart manufacturing readiness assessment methodology and requirements
CAN/CSA-ISO 14971	Medical Devices – Application of Risk Management to Medical Devices
CAN/CSA-CEI/IEC 62304	Medical device software – Software life cycle processes

Issue 7 —
Guidance on trustworthiness, ethical and societal use of data

ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO 10711	Intelligent Transport Systems – Interface Protocol and Message Set Definition between Traffic Signal Controllers and Detectors
ISO 12655	Energy performance of buildings – Presentation of measured energy use of buildings
ISO 13790	Energy performance of buildings – Calculation of energy use for space heating and cooling
ISO TR 17755	Fire safety – Overview of national fire statistics practices – First Edition
ISO TS 14048	Environmental Management – Life Cycle Assessment – Data Documentation Format – First Edition
ISO/IEC 19795-1	Information technology – Biometric performance testing and reporting – Part 1: Principles and framework
ISO/IEC 29155-1	Systems and software engineering – Information technology project performance benchmarking framework – Part 1: Concepts and definitions
ISO/IEC 29155-4	Systems and software engineering – Information technology project performance benchmarking framework Part 4: Guidance for data collection and maintenance
ISO/TS 14048	Environmental management – Life cycle assessment – Data documentation format
ASTM E2129	Standard Practice for Data Collection for Sustainability Assessment of Building Products
ASTM E2166	Standard Practice for Organizing and Managing Building Data
ASTM E2797	Standard Practice for Building Energy Performance Assessment for a Building Involved in a Real Estate Transaction
DIN SPEC 91367	Urban mobility data collection for real-time applications; Text in English
ETSI GS OSG 001	Open Smart Grid Protocol (OSGP) – V1.1.1
IEEE 1616	Motor Vehicle Event Data Recorders (MVEDRs)
IEEE 1856	Framework for Prognostics and Health Management of Electronic Systems
ITU-R RS.1859	Use of remote sensing systems for data collection to be used in the event of natural disasters and similar emergencies
ITU-R SA.1164-4	Sharing and coordination criteria for service links in data collection systems using GSO satellites in the Earth exploration-satellite and meteorological-satellite services
ITU-R SA.1627	Telecommunication requirements and characteristics of EESS and MetSat service systems for data collection and platform location – Question ITU-R 142/7
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing – Study Group 17
ITU-T Y.3603	Big data – Requirements and conceptual model of metadata for data catalogue – Study Group 13
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
CEN 16234-1	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all sectors – Part 1: Framework
CEN 17161	Design for All – Accessibility following a Design for All approach in products, goods and services – Extending the range of users
ISO 26000	Guidance on social responsibility (ISO 26000:2010)

ISO/IEC TR 29196	Guidance for biometric enrolment
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap Part 2: Architectural components and maturity model
ISO/TR 16982	Ergonomics of human-system interaction – Usability methods supporting human-centered design
ISO/TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TR 22758	Biotechnology – Biobanking – Implementation guide for ISO 20387
ISO/TS 14265	Health Informatics – Classification of purposes for processing personal health information
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
ISO/TS 22220	Health informatics – Identification of subjects of health care
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being
DS DS/CWA 17145-1	Ethics assessment for research and innovation – Part 1: Ethics committee
GOST K32095	Analysing Design Thinking: Studies of Cross-Cultural Co-Creation
CLSI I/LA21-A2	Clinical Evaluation of Immunoassays; Approved Guideline – Second Edition; Vol. 28 No. 22
BSI BS 42020	Biodiversity – Code of practice for planning and development
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and information services
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach – CORR: May 30, 2018
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CLSI H26-A2	Validation, Verification, and Quality Assurance of Automated Hematology Analyzers; Approved Standard – Second Edition; Vol 30; No 14
ITU-T SERIES Y SUPP 45	ITU-T Y.4000 series – Smart sustainable cities – An overview of smart sustainable cities and the role of information and communication technologies – Study Group 20
DS DS-håndbog 107.2	Quality management and quality management systems – Part 2: The "ISO 9000 family"
CEN/TR 15592	Health services – Quality management systems – Guide for the use of EN ISO 9004:2000 in health services for performance improvement
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
IEEE 7000 Series	Model Process for Addressing Ethical Concerns During System Design
IEEE P2840	Standard for Responsible AI Licensing

Issue 8 —
Harmonization and interoperability of data practices/ open data

ISO 5479	Statistical Interpretation of Data – Tests for Departure from the Normal Distribution – First Edition
ISO/IEC 9646-3	Information technology – Open Systems Interconnection (OSI) – Conformance testing methodology and framework – Part 3: The Tree and Tabular Combined Notation (TTCN)
ISO/IEC TR 10171	Information technology – Telecommunications and information exchange between systems – List of standard data link layer protocols that utilize high-level data link control (HDLC) classes of procedures, list of standard XID format identifiers, list of standard mode-setting information field format identifiers, and list of standard user-defined parameter set identification values
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
ISO/IEC 20016-1	Information technology for learning, education and training – Language accessibility and human interface equivalencies (HIEs) in e-learning applications – Part 1: Framework and reference model for semantic interoperability
ITU-T H.812	Interoperability design guidelines for personal connected health systems: Services interface – Study Group 16
ITU-T H.830.1	Conformance of ITU-T H.810 personal health system: Services interface Part 1: Web services interoperability: Health & Fitness Service sender – Study Group 16
ITU-T H.830.10	Conformance of ITU-T H.810 personal health system: Services interface Part 10: hData Observation Upload: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.11	Conformance of ITU-T H.810 personal health system: Services interface Part 11: Questionnaires: Health & Fitness Service sender – Study Group 16
ITU-T H.830.12	Conformance of ITU-T H.810 personal health system: Services interface Part 12: Questionnaires: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.13	Conformance of ITU-T H.810 personal health system: Services interface Part 13: Capability Exchange: Health & Fitness Service sender – Study Group 16
ITU-T H.830.14	Conformance of ITU-T H.810 personal health system: Services interface Part 14: Capability Exchange: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.15	Conformance of ITU-T H.810 personal health system: Services interface Part 15: FHIR Observation Upload: Health & Fitness Service sender – Study Group 16
ITU-T H.830.16	Conformance of ITU-T H.810 personal health system: Services interface Part 16: FHIR Observation Upload: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.2	Conformance of ITU-T H.810 personal health system: Services interface Part 2: Web services interoperability: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.4	Conformance of ITU-T H.810 personal health system: Services interface Part 4: SOAP/ATNA: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.5	Conformance of ITU-T H.810 personal health system: Services interface Part 5: PCD-01 HL7 messages: Health & Fitness Service sender – Study Group 16
ITU-T H.830.7	Conformance of ITU-T H.810 personal health system: Services interface Part 7: Consent management: Health & Fitness Service sender – Study Group 16
ITU-T H.830.8	Conformance of ITU-T H.810 personal health system: Services interface Part 8: Consent Management: Health & Fitness Service receiver – Study Group 16
ITU-T H.830.9	Conformance of ITU-T H.810 personal health system: Services interface Part 9: hData Observation Upload: Health & Fitness Service sender – Study Group 16
ITU-T H.831	Conformance of ITU-T H.810 personal health devices: WAN interface Part 1: Web services interoperability: Sender – Study Group 16
ITU-T H.832	Conformance of ITU-T H.810 personal health devices: WAN interface Part 2: Web services interoperability: Receiver – Study Group 16
ITU-T H.834	Conformance of ITU-T H.810 personal health devices: WAN interface Part 4: SOAP/ATNA: Receiver – Study Group 16

ITU-T H.835	Conformance of ITU-T H.810 personal health devices: WAN interface Part 5: PCD-01 HL7 messages: Sender – Study Group 16
ITU-T H.836	Conformance of ITU-T H.810 personal health devices: WAN interface Part 6: PCD-01 HL7 messages: Receiver – Study Group 16
ITU-T H.837	Conformance of ITU-T H.810 personal health devices: WAN interface Part 7: Consent management: Sender – Study Group 16
ITU-T H.838	Conformance of ITU-T H.810 personal health devices: WAN interface Part 8: Consent Management: Receiver – Study Group 16
ITU-T Q.3954	oneM2M – Interoperability testing – Study Group 20
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data – First Edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TR 38502	Information technology – Governance of IT – Framework and model
ISO/IEC TR 38504	Governance of information technology – Guidance for principles-based standards in the governance of information technology
ISO/IEC TS 38501	Information technology – Governance of IT – Implementation guide
SNZ AS/NZS 8016	Governance of IT enabled projects

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

ISO/IEC 27560	Privacy technologies – Consent record information structure
ISO/IEC 38505-1:2017	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data
N/A	Joint Initiative for Global Standards Harmonization Health Informatics Document Registry and Glossary
N/A	New European Interoperability Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 103-4	Digital trust and identity – Part 4: Digital wallets
IEEE 1900.6-2011	IEEE Standard for Spectrum Sensing Interfaces and Data Structures for Dynamic Spectrum Access and other Advanced Radio Communication Systems
IEEE P2896	Standard for Open Data: Open Data Ontology
IEEE P1484.11.1	Standard for Learning Technology – Data Model for Content Object Communication
IEEE 1609.11-2010	IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS)
IEEE C37.118.2-2011	IEEE Standard for Synchrophasor Data Transfer for Power Systems
IEEE/IEC C37.111-2013	IEEE Standard Common Format for Transient Data Exchange (COMTRADE) for Power Systems
IEEE 1451.0-2007	IEEE Standard for a Smart Transducer Interface for Sensors and Actuators – Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats
IEEE 2418.2-2020	IEEE Standard for Data Format for Blockchain Systems
N/A	Statistics Canada Statistical Standards (Concepts, Classifications, and Variables)

N/A	Data Documentation Initiative (DDI) – The Data Documentation Initiative (DDI) is an international standard for describing the data produced by surveys and other observational methods in the social, behavioral, economic, and health sciences. Standards include, XKOS, DDI Lifecycle, DDI-Codebook and DDI-CDI
N/A	Data Catalog Vocabulary (DCAT) – An RDF vocabulary designed to facilitate interoperability between data catalogs

Issue 9 —
Data actor and data transaction roles

CEN EN 13608-3	Health informatics – Security for healthcare communication – Part 3: Secure data channels
SNZ AS/NZS 5478	Recordkeeping metadata property reference set (RMPRS)
CEN/TR 15449-3	Geographic information – Spatial data infrastructures – Part 3: Data centric view
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing – Study Group 17
ITU-T X.1641	Guidelines for cloud service customer data security – Study Group 17
ISO 16175.1	Information and documentation-Principles and functional requirements for records in electronic office environments Part 1: Overview and statement of principles
ISO 16175-1	Information and documentation – Principles and functional requirements for records in electronic office environments – Part 1: Overview and statement of principles
ASTM D4840	Standard Guide for Sample Chain-of-Custody Procedures
ASTM E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
ETSI TS 187 001	Network Technologies (NTECH); NGN SECurity (SEC); Requirements – V3.9.1
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
ISO/TS 8000-150	Data quality – Part 150: Master data: Quality management framework
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
N/A	EDPS Guidelines on the concepts of controller, processor and joint controllership under Regulation (EU) 2018/1725
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
IEEE 117-2015	IEEE Standard Test Procedure for Evaluation of Systems of Insulating Materials for Random-Wound AC Electric Machinery
IEEE P2957	Standard for a Reference Architecture for Big Data Governance and Metadata Management
IEEE P802.3cy	Standard for Ethernet Amendment: Physical Layer Specifications and Management Parameters for greater than 10 Gb/s Electrical Automotive Ethernet
IEEE 1588-2019	IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

IEEE P2144.2	This standard defines the functional requirements in data compliance, governance and risk management in the operational process for Blockchain-based IoT data management systems
IEEE P802.1CBcv	Draft Standard for Local and metropolitan area networks – Frame Replication and Elimination for Reliability Amendment: Information Model, YANG Data Model and Management Information Base Module
IEEE P2418.2	The standard establishes data format requirements for a blockchain system (s).

Issue 10 —
Secondary use of data

DS DS/CWA 17145-1	Ethics assessment for research and innovation – Part 1: Ethics committee
ISO/IEC 29184	Information technology – Online privacy notices and consent – First edition
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements
CSA CSA-Q830-03	Model Code for the Protection of Personal Information – Second Edition
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
DS DS/CWA 14355	Guidelines for the implementation of Secure Signature-Creation Devices
ETSI TR 102 458	Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456) – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
IEC 61970-405	Energy management system application program interface (EMS-API) – Part 405: Generic Eventing and Subscription (GES)
IEC 62541-8	OPC unified architecture – Part 8: Data access – Edition 3.0
ISO 19115.1	Geographic information-Metadata Part 1: Fundamentals – Incorporating Amendment No. 1: June 2018
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO 19132	Geographic information – Locationbased services – Reference model
ISO/IEC 7816-11	Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods - Second Edition
ISO/IEC TR 24729-4	Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security – First Edition
ISO/IEC 24791-5	Information technology – Radio frequency identification (RFID) for item management – Software system infrastructure – Part 5: Device interface
ISO/IEC 9579-04	Information technology – Remote database access for SQL with security enhancement
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ETSI TS 102 342	Digital Enhanced Cordless Telecommunications (DECT); Cordless multimedia communication system; Open Data Access Profile (ODAP) – V1.2.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
ETSI TS 183 064	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN integrated IPTV subsystem stage 3 specification – V3.4.1; Includes Diskette
IEEE 1619.2	Wide-Block Encryption for Shared Storage Media – IEEE Computer Society
IEC 62628	Guidance on software aspects of dependability – Edition 1.0
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability – First Edition
ISO/IEC 25024	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of data quality

IEEE 1232.1	Trial Use – Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE): Data and Knowledge Specification
IEEE STDVA24228	BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP
ITU-T X.1602	Security requirements for software as a service application environments – Study Group 17
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derived requirements – First Edition
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – First Edition
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO/IEC TS 19249	Information technology – Security techniques – Catalogue of architectural and design principles for secure products, systems and applications
ISO/IEC 23751	Information technology – Cloud computing and distributed platforms – Data sharing agreement (DSA) framework
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use
ISO 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO 26000	Guidance on social responsibility
IWA 26:2017	Using ISO 26000:2010 in management systems
IWA 27 – sharing economy (TC 324)	Guiding principles and framework for the sharing economy
ISO/AWI 31700	Consumer protection – Privacy by design for consumer goods and services
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
IEEE P2933	Standard for clinical IoT Data & Devices interoperability with TIPPSS
IEEE P2876	Recommended Practice for Inclusion, Dignity and Privacy in Online Gaming
IEEE P7002	Data Privacy Process
IEEE P7012	Standard for Machine Readable Personal Privacy Terms
IEEE 2410	IEEE Standard for Biometric Open Protocol
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent: Component Overview and Conformance Profile v1.0

Working Group 2:
Data Collection, Organization, and Grading

Issue 11 —
Data Collection

NSC 120810000	Safety Metrics
ISO/TS 14048	Environmental Management – Life Cycle Assessment – Data Documentation Format – First Edition
ITU-R SA.1627	Telecommunication requirements and characteristics of EESS and MetSat service systems for data collection and platform location – Question ITU-R 142/7
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model
ITU-T SERIES Y SUPP 50	ITU-T Y.3650-series – Use case and application scenario for big-data-driven networking – Study Group 13
ITU-T Y.2618	The M interface in public packet telecommunication data networks – Study Group 13
ITU-T Y.2619	Operation, administration and maintenance functions and mechanisms for the public packet telecommunication data network (PTDN) – Study Group 13
ITU-T Y.2620	T interface for the public packet telecommunication data network – Study Group 13
ITU-T Y.3071	Data aware networking (information centric networking) – Requirements and capabilities – Study Group 13
ITU-T Y.3174	Framework for data handling to enable machine learning in future networks including IMT-2020 – Study Group 13
ITU-T Y.3505	Cloud computing – Overview and functional requirements for data storage federation – Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ITU-T Y.3604	Big data – Overview and requirements for data preservation – Study Group 13
ITU-T Y.3650	Framework of big-data-driven networking – Study Group 13
ITU-T Y.3651	Big-data-driven networking – mobile network traffic management and planning – Study Group 13
ITU-T Y.4461	Framework of open data in smart cities – Study Group 20
ITU-T Y.4468	Minimum set of data transfer protocol for automotive emergency response system – Study Group 20
ITU-T Y.4467	Minimum set of data structure for automotive emergency response system – Study Group 20
ITU-T SERIES Y SUPP 40	Big data standardization roadmap – Study Group 13
ITU-T SERIES Y SUPP 48	Proof-of-concept for data service using information centric networking in IMT-2020 – Study Group 13
ISO/IEC 29161	Information technology – Data structure – Unique identification for the Internet of Things – First Edition
ITU-T Y.2068	Functional framework and capabilities of the Internet of things – Study Group 13
ITU-T Y.3603	Big data – Requirements and conceptual model of metadata for data catalogue – Study Group 13
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ISO/IEC 23006-4	Information technology – Multimedia service platform technologies – Part 4: Elementary services – Second Edition

DS DS/CWA 16385	Interoperability of Registries
ISO/IEC 12034-1	Information technology – Archive eXchange Format (AXF) – Part 1: Structure and semantics – First Edition
BSI BS 17898	Code of practice for the management of observed hydrometric data
ISO/IEC 12785-2	Information technology – Learning, education, and training – Content packaging – Part 2: XML binding – First Edition
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CSA Z8003	Health care design research and evaluation

Issue 12 —
Data systems management

DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
ETSI GS ZSM 002	Zero-touch network and Service Management (ZSM); Reference Architecture – V1.1.1
ISO 37156	Smart community infrastructures – Guidelines on data exchange and sharing for smart community infrastructures
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO/IEC 27034-3	Information technology – Application security Part 3: Application security management process
ITU-T M.3041	Framework of smart operation, management and maintenance – Study Group 2
ITU-T M.3363	Requirements for data management in the telecommunication management network – Study Group 2
ITU-T Y.3604	Big data – Overview and requirements for data preservation – Study Group 13
IEC 62974-1	Monitoring and measuring systems used for data collection, gathering and analysis – Part 1: Device requirements
ISO/IEC 29155-4	Systems and software engineering – Information technology project performance benchmarking framework Part 4: Guidance for data collection and maintenance
ISO 26162	Systems to manage terminology, knowledge and content – Design, implementation and maintenance of terminology management systems
SAE GEIA-859A	Data Management – Formerly TechAmerica GEIA-859 REV A
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
SAE GEIA-HB-859	Implementation Guide for Data Management – Formerly TechAmerica GEIA-HB-859
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing – First Edition
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13

ISO/IEC TR 10032	Information technology – Reference Model of Data Management
ISO/IEC 10164-2	Information technology – Open Systems Interconnection – Systems Management: State Management Function AMENDMENT 1 : Implementation conformance statement proformas TECHNICAL CORRIGENDUM 1 – First Edition
ASTM E2842	Standard Guide for Credentialing for Access to an Incident or Event Site
ISO/IEC 10164-1	Information Technology – Open Systems Interconnection – Systems Management: Object Management Function – First Edition; Amendment: 5/15/1996; Corrigendum: 12/15/1996

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data

Issue 13 — Discoverability of the data

ANSI INCITS 284	Information Technology – Identification Cards – Health Care Identification Cards
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
IEC 62541-8	OPC unified architecture – Part 8: Data Access
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 24091	Information technology – Power efficiency measurement specification for data center storage – First edition
ISO/IEC 7816-11	Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods – Second Edition
ISO/IEC 9579-04	Information technology – Remote database access for SQL with security enhancement
ISO/TR 17424	Intelligent transport systems – Cooperative systems – State of the art of Local Dynamic Maps concepts
ISO 19115.1	Geographic information-Metadata Part 1: Fundamentals – Incorporating Amendment No. 1: June 2018
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
IEC TS 61850-7-7	Communication networks and systems for power utility automation – Part 7-7: Machine-processable format of IEC 61850-related data models for tools – Edition 1.0
ISO/IEEE 11073-10101	Health informatics – Point-of-care medical device communication – Part 10101: Nomenclature AMENDMENT 1: Additional definitions – First Edition
CLSI AUTO16	Next-Generation In Vitro Diagnostic Instrument Interface – 1st Edition; Volume 39; Number 4
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ISO 20078-3	Road vehicles – Extended vehicle (ExVe) web services – Part 3: Security
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
CEN EN 16931-1	Electronic invoicing – Part 1: Semantic data model of the core elements of an electronic invoice – Incorporates Amendment A1: 2019
DIN CEN/TS 17262	Personal identification – Robustness against biometric presentation attacks – Application to European Automated Border Control; English version CEN/TS 17262:2018
DS DS/CEN/TR 16931-4	Electronic invoicing – Part 4: Guidelines on interoperability of electronic invoices at the transmission level

DS DS/CEN/TS 17262	Personal identification – Robustness against biometric presentation attacks – Application to European Automated Border Control
ETSI EN 300 175-4	Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 4: Data Link Control (DLC) layer – V2.8.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 102 563	Digital Audio Broadcasting (DAB); DAB+ audio coding (MPEG HE-AACv2) – V2.1.1
ETSI TS 103 466	Digital Audio Broadcasting (DAB); DAB audio coding (MPEG Layer II) – V1.2.1
ISO 17427-1	Intelligent transport systems – Cooperative ITS – Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s) (ISO 17427-1:2018)
ISO 17892-12	Geotechnical investigation and testing – Laboratory testing of soil – Part 12: Determination of liquid and plastic limits (ISO 17892-12:2018)
ISO 18185-4	Freight containers – Electronic seals – Part 4: Data protection
ISO 24534-3	Intelligent transport systems – Automatic vehicle and equipment identification – Electronic registration identification (ERI) for vehicles – Part 3: Vehicle data – Second Edition
ISO 13527	Space data and information transfer systems – XML formatted data unit (XFDU) structure and construction rules – First Edition
ISO 14199	Health informatics – Information models – Biomedical Research Integrated Domain Group (BRIDG) Model
ISO 14825	Intelligent transport systems – Geographic Data Files (GDF) – GDF5.0
ISO 15489-1	Information and documentation – Records management – Part 1: Concepts and principles
ISO 15836-1	Information et documentation – L'ensemble des éléments de métadonnées Dublin Core – Partie 1 : éléments principaux
ISO 15836-2	Information and documentation – The Dublin Core metadata element set Part 2: DCMI Properties and classes
ISO 16684-1	Graphic technology – Extensible metadata platform (XMP) Part 1: Data model, serialization and core properties
ISO 16684-2	Graphic technology – Extensible metadata platform (XMP) Part 2: Description of XMP schemas using RELAX NG
ISO 17316	Information and documentation – International standard link identifier (ISLI)
ISO 17972-1	Graphic technology – Colour data exchange format – Part 1: Relationship to CxF3 (CxF/X)
ISO 17972-2	Graphic technology – Colour data exchange format (CxF/X) – Part 2: Scanner target data (CxF/X-2)
ISO 17972-3	Graphic technology – Colour data exchange format (CxF/X) – Part 3: Output target data (CxF/X-3) – First Edition
ISO 19109	Geographic information – Rules for application schema
ISO 19111	Geographic information – Referencing by coordinates
ISO 19115.2	Geographic information – Metadata Part 2: Extensions for acquisition and processing
ISO 19115-2	Geographic information – Metadata – Part 2 : extensions for acquisition and processing
ISO 19130.2	Geographic information-Imagery sensor models for geopositioning Part 2: SAR, InSAR, lidar and sonar
ISO 19130-1	Geographic information – Imagery sensor models for geopositioning – Part 1: Fundamentals
ISO 19139.2	Geographic information-Metadata – XML schema implementation Part 2: Extensions for imagery and gridded data
ISO 19150-4	Geographic information – Ontology – Part 4: Service ontology
ISO 19159.1	Geographic information – Calibration and validation of remote sensing imagery sensors and data Part 1: Optical sensors

ISO 19159.3	Geographic information – Calibration and validation of remote sensing imagery sensors and data Part 3: SAR/InSAR
ISO 19160.1	Addressing Part 1: Conceptual model
ISO 19160-1	Addressing – Part 1: Conceptual model
ISO 19162	Geographic information – Well-known text representation of coordinate reference systems
ISO 19165.1	Geographic information – Preservation of digital data and metadata Part 1: Fundamentals
ISO 19165-1	Geographic information – Preservation of digital data and metadata Part 1: Fundamentals
ISO 19289	Air quality – Meteorology – Siting classifications for surface observing stations on land – First Edition
ISO 19445	Graphic technology – Metadata for graphic arts workflow – XMP metadata for image and document proofing
ISO 19593-1	Graphic technology – Use of PDF to associate processing steps and content data – Part 1: Processing steps for packaging and labels
ISO 20614	Information and documentation – Data exchange protocol for interoperability and preservation
ISO 20616-2	Graphic technology – File format for quality control and metadata Part 2: Print Quality eXchange (PQX)
ISO 2108	Information and documentation – International Standard Book Number (ISBN)
ISO 21812-1	Graphic technology – Print product metadata for PDF files Part 1: Architecture and core requirements for metadata
ISO 23081-1	Information and documentation – Records management processes – Metadata for records – Part 1 : principles
ISO 24097-1	Intelligent transport systems – Using web services (machine-machine delivery) for ITS service delivery – Part 1: Realization of interoperable web services – Second Edition
ISO 24619	Language resource management – Persistent identification and sustainable access (PISA) (ISO 24619:2011)
ISO 24622-2	Language resource management – Component metadata infrasctructure (CMDI) Part 2: Component metadata specification language
ISO 25577	Information and documentation – MarcXchange
ISO 26324	Information and documentation – Digital object identifier system
ISO 27730	Information and documentation – International standard collection identifier (ISCI)
ISO 28258	Soil quality – Digital exchange of soil-related data – Incorporates Amendment A1: 2019
ISO 28500	Information and documentation – WARC file format
ISO 639-4	Codes for the representation of names of languages – Part 4: General principles of coding of the representation of names of languages and related entities, and application guidelines
ISO 8	Information and documentation – Presentation and identification of periodicals
ISO TR 13054	Knowledge management of health information standards – First Edition
ISO TR 13128	Health informatics – Clinical document registry federation – First Edition
ISO TR 17321-2	Graphic technology and photography – Colour characterization of digital still cameras (DSCs) – Part 2: Considerations for determining scene analysis transforms – First Edition
ISO TR 23081-3	Information and documentation – Managing metadata for records – Part 3: Self-assessment method – First Edition
ISO TR 24097-2	Intelligent transport systems – Using web services (machine-machine delivery) for ITS service delivery – Part 2: Elaboration of interoperable web services' interfaces – First Edition
ISO TR 24097-3	Intelligent transport systems – Using web services (machine-machine delivery) for ITS service delivery – Part 3: Quality of service – First Edition
ISO TS 13972	Health informatics – Detailed clinical models, characteristics and processes – First Edition
ISO TS 15926-12	Industrial automation systems and integration – Integration of life-cycle data for process plants including oil and gas production facilities – Part 12: Life-cycle integration ontology represented in Web Ontology Language (OWL)

ISO TS 17439	Health informatics – Development of terms and definitions for health informatics glossaries – First Edition
ISO TS 17948	Health informatics – Traditional Chinese medicine literature metadata – First Edition
ISO TS 19115-3	Geographic information – Metadata – Part 3: XML schema implementation for fundamental concepts – First Edition
ISO TS 19159-2	Geographic information – Calibration and validation of remote sensing imagery sensors and data – Part 2: Lidar – First Edition
ISO TS 19159-3	Geographic information – Calibration and validation of remote sensing imagery sensors and data – Part 3: SAR/InSAR – First edition
ISO TS 20428	Health informatics – Data elements and their metadata for describing structured clinical genomic sequence information in electronic health records – First Edition
ISO TS 21526	Health informatics – Metadata repository requirements (MetaRep) – First edition
ISO/IEC 11179-1	Information technology – Metadata registries (MDR) – Part 1: Framework – Third Edition
ISO/IEC 11179-5	Information technology – Metadata registries (MDR) – Part 5: Naming principles – Third Edition
ISO/IEC 11179-6	Information technology – Metadata registries (MDR) – Part 6: Registration – Third Edition
ISO/IEC 14957	Information technology – Representation of data element values – Notation of the format – Second Edition
ISO/IEC 15444-2	Information technology – JPEG 2000 image coding system: Extensions – Incorporates Corrigendum 3: December 2006; Corrigendum 4: December 2010
ISO/IEC 15444-5	Information technology – JPEG 2000 image coding system: Reference software – Second Edition
ISO/IEC 15444-6	Information technology – JPEG 2000 image coding system – Part 6: Compound image file format – Second Edition
ISO/IEC 15444-8	Information technology – JPEG 2000 image coding system – Part 8: Secure JPEG 2000
ISO/IEC 16500-6	Information technology – Generic digital audio-visual systems – Part 6: Information representation
ISO/IEC 19566-5	Information technologies – JPEG systems – Part 5: JPEG universal metadata box format (JUMBF) – First edition
ISO/IEC 19763-5	Information technology – Metamodel framework for interoperability (MFI) – Part 5: Metamodel for process model registration – First Edition
ISO/IEC 19763-6	Information technology – Metamodel framework for interoperability (MFI) – Part 6: Registry Summary – First Edition
ISO/IEC 19788-7	Information technology – Learning, education and training – Metadata for learning resources – Part 7: Bindings – First edition
ISO/IEC 19788-8	Information technology – Learning, education and training – Metadata for learning resources – Part 8: Data elements for MLR records – First Edition
ISO/IEC 19788-9	Information technology – Learning, education and training – Metadata for learning resources – Part 9: Data elements for persons – First Edition
ISO/IEC 19794-13	Information technology – Biometric data interchange formats – Part 13: Voice data – First Edition
ISO/IEC 20248	Information technology – Automatic identification and data capture techniques – Data structures – Digital signature meta structure – First Edition
ISO/IEC 20944-2	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 2: Coding bindings – First Edition
ISO/IEC 20944-3	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 3: API bindings – First Edition
ISO/IEC 20944-4	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 4: Protocol bindings – First Edition
ISO/IEC 20944-5	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) – Part 5: Profiles – First Edition
ISO/IEC 21000-22	Information technology – Multimedia framework (MPEG-21) – Part 22: User Description

ISO/IEC 22602	Informationsteknologi – Læring, uddannelse og træning – Model for kompetencer udtrykt i metadata til læringsressourcer (MLR)
ISO/IEC 23000-22	Information technology – Multimedia application format (MPEG-A) – Part 22: Multi-image application format (MIAF) – First edition
ISO/IEC 23001-10	Information technology – MPEG systems technologies – Part 10: Carriage of timed metadata metrics of media in ISO base media file format – Second edition
ISO/IEC 23001-11	Information technology – MPEG systems technologies – Part 11: Energy-efficient media consumption (green metadata) – Second edition
ISO/IEC 23001-13	First edition
ISO/IEC 23001-7	Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files – Third Edition
ISO/IEC 23005-4	Information technology – Media context and control – Part 4: Virtual world object characteristics – Fourth Edition
ISO/IEC 23008-12	Information technology – High efficiency coding and media delivery in heterogeneous environments – Part 12: Image File Format – First Edition
ISO/IEC 23008-3	Information technology – High efficiency coding and media delivery in heterogeneous environments – Part 3: 3D audio AMENDMENT 1: Audio metadata enhancements – Second edition
ISO/IEC 23092-3	Information technology – Genomic information representation – Part 3: Metadata and application programming interfaces (APIs) – First edition
ISO/IEC 24800-5	Information technology – JPSearch – Part 5: Data interchange format between image repositories – First Edition
ISO/IEC 29500-2	Information technology – Document description and processing languages – Office Open XML File Formats – Part 2: Open Packaging Conventions – Third Edition
ISO/IEC 40260	Information technology – W3C Web Services Addressing 1.0 – Metadata – First Edition; Includes Access to Additional Content
ISO/IEC TR 11179-2	Information technology – Metadata registries (MDR) – Part 2: Classification – First edition
ISO/IEC TR 15938-11	Information technology – Multimedia content description Interface – Part 11: MPEG-7 profile schemas
ISO/IEC TR 15938-8	Information technology – Multimedia content description interface – Part 8: Extraction and use of MPEG-7 descriptions
ISO/IEC TR 19583-1	Information technology – Concepts and usage of metadata – Part 1: Metadata concepts – First edition
ISO/IEC TR 19583-22	Information technology – Concepts and usage of metadata – Part 22: Registering and mapping development processes using ISO/IEC 19763 – First Edition
ISO/IEC TR 20943-1	Information technology Procedures for achieving metadata registry (MDR) content consistency Part 1: Data elements – First Edition
ISO/IEC TR 20943-3	Information technology Procedures for achieving metadata registry content consistency Part 3: Value domains – First Edition
ISO/IEC TR 20943-5	Information technology – Procedures for achieving metadata registry content consistency – Part 5: Metadata mapping procedure – First Edition
ISO/IEC TR 20943-6	Information technology – Procedures for achieving metadata registry content consistency – Part 6: Framework for generating ontologies – First Edition
ISO/IEC TR 21000-11	Information technology – Multimedia framework (MPEG-21) – Part 11: Evaluation Tools for Persistent Association Technologies
ISO/IEC TS 11179-30	Information technology – Metadata registries (MDR) – Part 30: Basic attributes of metadata – First edition
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems, software, and services information – First Edition
ISO/TR 23081-3	Information and documentation. Managing metadata for records. Self-assessment method – Hardcopy Only – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide

ISO/TS 19115-3	Geographic information – Metadata Part 3: XML schema implementation for fundamental concepts
ISO/TS 19130	Geographic information – Imagery sensor models for geopositioning
ISO/TS 19130-2	Geographic information – Imagery sensor models for geopositioning – Part 2: SAR, InSAR, lidar and sonar
ISO/TS 19139	Geographic information – Metadata – XML schema implementation
ISO/TS 19139-2	Geographic information – Metadata – XML schema implementation Part 2: Extensions for imagery and gridded data
ITU-R BS.2076-2	Audio Definition Model
ITU-R BS.2088-1	Long-form file format for the international exchange of audio programme materials with metadata
ITU-T F.750	Metadata framework
ITU-T T.804	Information technology – JPEG 2000 image coding system: Reference software – Study Group 16
ITU-T T.805	(Pre-Published) Information technology – JPEG 2000 image coding system: Compound image file format
ITU-T T.808	Information technology – JPEG 2000 image coding system: Interactivity tools, APIs and protocols
ITU-T X.1276	Authentication step-up protocol and metadata Version 1.0 – Study Group 17
ITU-T Y.3603	Big data – Requirements and conceptual model of metadata for data catalogue – Study Group 13
ULC CAN/ULC-S316-14	STANDARD FOR PERFORMANCE OF VIDEO SURVEILLANCE SYSTEMS – First Edition
ISO/IEC TR 29163-1	Information technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition – Part 1: Overview Version 1.1 – Third edition
ITU-T X.1255	Framework for discovery of identity management information – Study Group 17
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derived requirements – First Edition
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
ISO/IEC TR 29163-2	Information technology – Sharable Content Object Reference Model (SCORM) 2004 3rd Edition – Part 2: Content Aggregation Model Version 1.1 – Third Edition
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services
ISO/IEC 30141	Internet of Things (IoT) – Reference Architecture
ISO/IEC 30118-2	Information technology – Open Connectivity Foundation (OCF) Specification Part 2: Security specification
ISO/IEC 23271	Information technology Common Language Infrastructure – Adopted by INCITS
ISO/IEC 30118-1	Information technology – Open Connectivity Foundation (OCF) Specification Part 1: Core specification
ISO 16175.2	Information and documentation – Principles and functional requirements for records in electronic office environments Part 2: Guidelines and functional requirements for digital records management systems
ISO 16175-2	Information and documentation – Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for digital records management systems
ISO/IEC 23270	Information technology C# Language Specification – Adopted by INCITS
ISO/IEC 19763-1	Information technology – Metamodel framework for interoperability (MFI) – Part 1: Framework
ANSI INCITS 530	Information Technology – Architecture for Managed Computing Systems
ISO/IEC 18384-1	Information technology – Reference Architecture for Service Oriented Architecture (SOA RA) Part 1: Terminology and concepts for SOA
ISO/IEC TR 30102	Information technology – Distributed Application Platforms and Services (DAPS) – General technical principles of Service Oriented Architecture
ISO/IEC TR 22417	Information technology – Internet of things (IOT) – IOT use cases

BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach – CORR: May 30, 2018
ISO/IEC 23271	Information technology – Common Language Infrastructure (CLI) – Third Edition
IEC 62656-1	Standardized product ontology register and transfer by spreadsheets – Part 1: Logical structure for data parcels – Edition 1.0
IEC 82045-1	Document Management – Part 1: Principles and Methods – Edition 1.0
ISO 19115	Geographic information Metadata
ISO/IEC 11179-3	Information technology – Metadata registries (MDR) – Part 3: Registry metamodel and basic attributes – Third Edition
ISO/IEC 20802-1	Information technology – Open data protocol (OData) v4.0 Part 1: Core – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CIOSC/PAS 100-4:2020	Data governance – Part 4: Specification for Scalable Remote Access Infrastructure
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 106-1	Discovery and management of Digital Twins for built environments – Part 1: Discovery
IEEE 1667-2018	IEEE Standard for Discovery, Authentication, and Authorization in Host Attachments of Storage Devices
IEEE P2957	Standard for a Reference Architecture for Big Data Governance and Metadata Management
IEEE P1951.1	Standard for Smart City Component Systems Discovery and Semantic Exchange of Objectives
IEEE P1752	IEEE Approved Draft Standard for Mobile Health Data
N/A	Statistics Canada Statistical Standards (Concepts, Classifications, and Variables)
N/A	Data Documentation Initiative (DDI) – The Data Documentation Initiative (DDI) is an international standard for describing the data produced by surveys and other observational methods in the social, behavioral, economic, and health sciences. Standards include, XKOS, DDI Lifecycle, DDI-Codebook and DDI-CDI
N/A	Data Catalog Vocabulary (DCAT) – An RDF vocabulary designed to facilitate interoperability between data catalogs

Issue 14 — Data Linkage

API BULL 1178	Integrity Data Management and Integration – FIRST EDITION
ETSI TR 103 290	Machine-to-Machine communications (M2M); Impact of Smart City Activity on IoT Environment – V1.1.1
ETSI TR 103 376	SmartM2M; IoT LSP use cases and standards gaps – V1.1.1
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms – V1.1.2
ETSI TS 118 101	Functional Architecture – V2.10.0; oneM2M TS-0001 version 2.10.0 Release 2
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information

ISO TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations – First Edition
ISO 22857	Health informatics – Guidelines on data protection to facilitate transborder flows of personal health data
ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002 (ISO 27799:2016)
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – First Edition
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derived requirements – First Edition
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability – First Edition
ISO/IEC 20006.1	Information technology for learning, education and training – Information model for competency Part 1: Competency general framework and information model
ISO/IEC 20006-1	Information technology for learning, education and training – Information model for competency – Part 1: Competency general framework and information model – First Edition
ISO/IEC 21823-1	Internet of things (IoT) – Interoperability for iot systems Part 1: Framework
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TR 20547-5	Information technology – Big data reference architecture – Part 5: Standards roadmap – First edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TS 19763-13	Information technology – Metamodel framework for interoperability (MFI) – Part 13: Metamodel for form design registration – First Edition
ISO/IEC/IEEE 24748-7	Systems and software engineering – Life cycle management Part 7: Application of systems engineering on defense programs
ITU-T X.1363	(Pre-Published) Technical framework of personally identifiable information (PII) handling in Internet of things (IoT) environment
ITU-T X.1040	Security reference architecture for lifecycle management of e-commerce business data – Study Group 17
ITU-T SERIES Y SUPP 40	Big data standardization roadmap – Study Group 13
ITU-T X.814	Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Confidentiality Framework – Data Networks and Open System Communications Security 25 pp
ITU-T Y.4203	Requirements of things description in the Internet of things – Study Group 20
ITU-T Z.100 ANNEX F1	Specification and Description Language – Overview of SDL-2010 Annex F1: SDL-2010 formal definition: General overview – Study Group 17
ITU-T Z.100 ANNEX F3	Specification and Description Language – Overview of SDL-2010 Annex F3: SDL-2010 formal definition: Dynamic semantics – Study Group 17

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

IEEE Std 1888.4-2016	IEEE Standard for Green Smart Home and Residential Quarter Control Network Protocol –
IEEE P2030	IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework

Issue 15 —
Manual tagging of data

ISO/IEC 19790	Information technology – Security techniques – Security requirements for cryptographic modules – Second Edition; Corrected version 12/15/2015
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operational environment – First Edition
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
BSI BS 5701-2	Guide to quality control and performance improvement using qualitative (attribute) data – Part 2: Fundamentals of standard attribute charting for monitoring, control and improvement
ISO 19731	Digital analytics and web analyses for purposes of market, opinion and social research – Vocabulary and service requirements – First Edition
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada

Issue 16 —
Metadata management

ISO/IEC 23001-13	Information technology – MPEG systems technologies – Part 13: Media orchestration
IEC 82045-1	Document Management – Part 1: Principles and Methods – Edition 1.0
IEC 82045-2	Document management – Part 2: Metadata elements and information reference model
IEEE 1484.12.3	Standard for Learning Technology – Extensible Markup Language (XML) Schema Definition Language Binding for Learning Object Metadata – IEEE Computer Society
IEEE COMP	IEEE Standard Computer Dictionary Compilation of IEEE Standard Computer Glossaries – IEEE Computer Society Document
ISO 17369	Statistical data and metadata exchange (SDMX) – First Edition
ISO 24622-1	Language resource management – Component Metadata Infrastructure (CMDI) Part 1: The Component Metadata Model
BIS IS 15992	Information and Documentation – The Dublin Core Metadata Element Set
ISO 15836	Information and documentation – The Dublin Core metadata element set TECHNICAL CORRIGENDUM 1 – Second Edition
ISO 15836-1	Information and documentation – The Dublin Core metadata element set – Part 1: Core elements – First Edition
ISO 15836-2	Information and documentation – The Dublin Core metadata element set – Part 2: DCMI Properties and classes – First edition
SNZ SA/SNZ HB 168	Document control
ISO/IEC 11179-1	Information technology – Metadata registries (MDR) – Part 1: Framework – Third Edition
ISO 24622-2	Language resource management – Component metadata infrasctructure (CMDI) – Part 2: Component metadata specification language – First edition
IEEE STDVA24228	BIG DATA GOVERNANCE AND METADATA MANAGEMENT: STANDARDS ROADMAP
ISO/IEC 11179-6	Information technology – Information technology – Metadata registries (MDR) – Part 6: Registration
ETSI GR NFV-SEC 003	Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance – V1.2.1
ASTM E2468	Standard Practice for Metadata to Support Archived Data Management Systems

ISO/IEC TR 20943-6	Information technology – Procedures for achieving metadata registry content consistency – Part 6: Framework for generating ontologies – First Edition
ISO/IEC 11179-2	Information technology Metadata registries (MDR) Part 2: Classification – Second Edition
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
IEEE P2957	Standard for a Reference Architecture for Big Data Governance and Metadata Management
IEEE P2881	Standard for Learning Metadata
IEEE P4002	Standard for Synthetic Aperture Radar Metadata Content
IEEE P4003	IEEE Draft Standard for Global Navigation Satellite System-Reflectometry (GNSS-R) Data and Metadata Content
IEEE IC17-006	Big Data Governance and Metadata Management
N/A	Statistics Canada Statistical Standards (Concepts, Classifications, and Variables)
N/A	Data Documentation Initiative (DDI) – The Data Documentation Initiative (DDI) is an international standard for describing the data produced by surveys and other observational methods in the social, behavioral, economic, and health sciences. Standards include, XKOS, DDI Lifecycle, DDI-Codebook and DDI-CDI
N/A	Data Catalog Vocabulary (DCAT) – An RDF vocabulary designed to facilitate interoperability between data catalogs

Issue 17 —
Organizational Data policy strategies and risks management

ANSI X9.111	Penetration Testing within the Financial Services Industry – ASCX9
ANSI X9.100-181	Specification for TIFF Image Format for Image Exchange
API BULL 1178	Integrity Data Management and Integration – FIRST EDITION
API PUBL 353	Managing Systems Integrity of Terminal and Tank Facilities Managing the Risk of Liquid Petroleum Releases – First Edition
API PUBL 4620	International Oil Spill Conference Proceedings Achieving and Maintaining Preparedness
ASCE GSP 98	PAVEMENT SUBGRADE, UNBOUND MATERIALS, AND NONDESTRUCTIVE TESTING
ASHRAE HVAC APPLICATIONS SI HANDBOOK	2019 ASHRAE Handbook HVAC Applications SI Edition
ASTM MNL19	Manual on the Building of Materials Databases
ASTM E2842	Standard Guide for Credentialing for Access to an Incident or Event Site
ASTM F3286	Standard Guide for Cybersecurity and Cyberattack Mitigation
ASTM F3449	Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems in Accordance with IMO Resolution MSC.428(98) – Cyber Risks and Challenges
ASTM E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)
ASTM E2147	Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems
ASTM MNL58	Petroleum Refining and Natural Gas Processing
AWWA G410	Business Practices for Operation and Management
BSI BS 70000	Medical physics, clinical engineering and associated scientific services in healthcare – Requirements for quality, safety and competence

BSI PD 7506	Linking Knowledge Management with other Organizational Functions and Disciplines: A Guide to Good Practice
BSI PD 8100	Smart cities overview – Guide
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code of practice for implementation of BS 10008-1
BSI PD 7505	Skills for Knowledge Working: A Guide to Good Practice
BSI PAS 197	Code of practice for cultural collections management
CEN/TR 15584	Characterisation of sludges – Guide to risk assessment especially in relation to use and disposal of sludges
CEN 17255-2	Stationary source emissions – Data acquisition and handling systems – Part 2: Specification of requirements on data acquisition and handling systems
CEN/TR 17370	Public transport – Operating raw data and statistics exchange
CEN/TS 17434	Ambient air – Determination of the particle number size distribution of atmospheric aerosol using a Mobility Particle Size Spectrometer (MPSS)
CEN EN 50518	Monitoring and Alarm Receiving Centre
CEN/TR 16674	Information technology – Analysis of privacy impact assessment methodologies relevant to RFID
CENELEC EN 50436-6	Alcohol interlocks – Test methods and performance requirements – Part 6 : data security
CENELEC EN 50491-12-1	General requirements for Home and Building Electronic Systems (HBES) and Building Automation and Control Systems (BACS) – Smart grid – Application specification – Interface and framework for customer – Part 12-1: Interface between the CEM and Home/Building Resource manager – General Requirements and Architecture
CENELEC EN 50600-3-1	Information technology – Data centre facilities and infrastructures – Part 3-1: Management and operational information
CLSI QMS22	Management of Paper-based and Electronic Laboratory Information – First Edition
DS DS/CWA 15847	Innovation, Coordination and Collaboration in Service Driven Manufacturing Supply Chains – Reference Model for Industrial Services
ETSI TS 187 001	Network Technologies (NTECH); NGN SECurity (SEC); Requirements – V3.9.1
ETSI GS ISI 002	Information Security Indicators (ISI); Event Model A security event classification model and taxonomy – V1.2.1
ETSI TR 102 659-1	GRID; Study of ICT Grid interoperability gaps; Part 1: Inventory of ICT Stakeholders – V1.2.1
GOST R 34.13	Information technology. Cryptographic data security. Block ciphers operation modes
IEC 62056-21	Electricity Metering – Data Exchange for Meter Reading, Tariff and Load Control – Part 21: Direct Local Data Exchange – Edition 1.0
IEC 62962	Particular requirements for load-shedding equipment (LSE)
IEC/IEEE 82079-1	Preparation of information for use (instructions for use) of products – Part 1: Principles and general requirements – Edition 2.0
IEC 62443-2-1	Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program – First Edition
IEC 60300-3-15	Dependability management Part 3-15: Application guide – Engineering of system dependability
IEEE 1232.1	Trial Use – Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE): Data and Knowledge Specification
IEEE 1685	IP-XACT, Standard Structure for Packaging, Integrating, and Reusing IP within Tool Flows – IEEE Computer Society
IEEE 1455	Standard for Message Sets for Vehicle/Roadside Communications
IEEE 1484.11.2	Learning Technology – ECMAScript Application Programming Interface for Content to Runtime Services Communication – IEEE Computer Society
IEEE 1914.1	Packet-based Fronthaul Transport Network – Includes Access to Additional Content

IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE ICICLE	IEEE IC INDUSTRY CONSORTIUM ON LEARNING ENGINEERING
ISO 8000-2	Data quality Part 2: Vocabulary
ISO/TS 8000-65	Data quality – Part 65: Data quality management: Process measurement questionnaire
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO/IEC 20547-3	Information technology – Big data reference architecture – Part 3: Reference architecture – First edition
ISO/IEC 38506	Information technology – Governance of IT – Application of ISO/IEC 38500 to the governance of IT enabled investments – First edition
ISO 14644-2	Cleanrooms and associated controlled environments – Part 2: Monitoring to provide evidence of cleanroom performance related to air cleanliness by particle concentration
ISO 14031	Environmental Management – Environmental Performance Evaluation – Guidelines
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 13211-1	Information technology – Programming languages – Prolog – Part 1: General core
ISO/IEC 19778-1	Information technology – Learning, education and training – Collaborative technology – Collaborative workplace – Part 1: Collaborative workplace data model
ISO/IEC 9075-2	Information technology – Database languages – SQL – Part 2: Foundation (SQL/Foundation) – Fifth Edition
ISO/IEC TS 18508	Information technology – Additional Parallel Features in Fortran – First Edition
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ISO 17427-1	Intelligent transport systems – Cooperative ITS – Part 1: Roles and responsibilities in the context of co-operative ITS architecture(s) (ISO 17427-1:2018)
ISO 17892-12	Geotechnical investigation and testing – Laboratory testing of soil – Part 12: Determination of liquid and plastic limits (ISO 17892-12:2018)
ISO TR 23791	Road vehicles – Extended vehicle (ExVe) web services – Result of the risk assessment on ISO 20078 series – First edition
ISO/TS 17427	Intelligent transport systems – Cooperative systems – Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems
ISO 15638-21	Intelligent transport systems – Framework for cooperative telematics applications for regulated commercial freight vehicles (TARV) – Part 21: Monitoring of regulated vehicles using roadside sensors and data collected from the vehicle for enforcement and other purposes
ISO/IEC TR 24729-4	Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security – First Edition
ISO 16598	Timber structures – Structural classification for sawn timber – First Edition
ISO TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles – First Edition
ISO 16919	Space data and information transfer systems – Requirements for bodies providing audit and certification of candidate trustworthy digital repositories – First Edition
ISO 22307	Financial services – Privacy impact assessment
ISO/IEC TS 33072	Information technology – Process assessment – Process capability assessment model for information security management
ISO/TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations
ISO/IEC 27002	Information technology – Security techniques – Code of practice for information security controls (ISO/IEC 27002:2013 including Cor 1:2014 and Cor 2:2015)
ISO/IEC 15504-6	Information technology – Process assessment – Part 6: An exemplar system life cycle process assessment model – First Edition
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles

ISO/HL7 27951 cd-rom	Health informatics – Common terminology services, release 1
ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC 27018	Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27017	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiable information protection
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation of virtualized servers – First Edition
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO 41001	Facility management – Management systems – Requirements with guidance for use – First Edition
ISO 30302	Information and documentation – Management systems for recordkeeping-Guidelines for implementation
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information – First Edition
ITU-T Y.2330	Requirements of next generation network evolution for supporting freedata service – Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T X.1040	Security reference architecture for lifecycle management of e-commerce business data – Study Group 17
ITU-T X.1086	Telebiometrics protection procedures – Part 1: A guideline to technical and managerial countermeasures for biometric data security – Study Group 17
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing – Study Group 17
ITU-T X.1641	Guidelines for cloud service customer data security – Study Group 17
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
NEMA MITA CSP 1	Cybersecurity for Medical Imaging
NEN NPR-CR 1832	CIM Systems Architecture – Enterprise model execution and integration services – Statement of requirements
SAE GEIA-859A	Data Management – Formerly TechAmerica GEIA-859 REV A
SAE GEIA-HB-649A	(R) Configuration Management Standard Implementation Guide
SAE GEIA-HB-859	Implementation Guide for Data Management – Formerly TechAmerica GEIA-HB-859
SAE PT-182	Integrated Vehicle Health Management – System of Systems Integration – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SNV SN CR 13694	Health informatics – Safety and Security Related Software Quality Standards for Healthcare (SSQS)
SNZ NZS 8153	Health Records
SNZ SA/SNZ HB 168	Document control
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
IEEE/ISO/IEC 29119-2-2013	ISO/IEC/IEEE International Standard – Software and systems engineering – Software testing – Part 2:Test processes

CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
n/a	Best Practice Guide to Applying Data Sharing Principles
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data

Issue 18 —
Data Quality and Fitness for Use Assessment

ISO/TS 8000-1	Data quality – Part 1: Overview
ISO/TS 8000-110	Data quality – Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specification
ISO TS 8000-311	Data quality – Part 311: Guidance for the application of product data quality for shape (PDQ-S) – First Edition
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO TS 8000-1	Data quality – Part 1: Overview – First Edition; Includes Access to Additional Content
ISO 8000-8	Data quality Part 8: Information and data quality: Concepts and measuring
ISO 17369	Statistical data and metadata exchange (SDMX) – First Edition
API BULL 1178	Integrity Data Management and Integration – FIRST EDITION
ISO/TS 14048-03	Environmental management – Life cycle assessment – Data documentation format – First Edition
ISO 8000-100	Data quality – Part 100: Master data: Exchange of characteristic data: Overview – First Edition
ISO/IEC 25012	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model – First Edition
ISO 8000-140	Data quality – Part 140: Master data: Exchange of characteristic data: Completeness – First Edition
ISO 8000-110	Data quality – Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specification – First Edition; Includes Access to Additional Content
ISO 8000-130	Data quality – Part 130: Master data: Exchange of characteristic data: Accuracy – First Edition
ISO 8000-116	Data quality Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 to authoritative legal entity identifiers
ISO 8000-2	Data quality – Part 2: Vocabulary – Third Edition
ISO/TS 8000-150	Data quality – Part 150: Master data: Quality management framework
ISO 8000-62	Data quality – Part 62: Data quality management: Organizational process maturity assessment: Application of standards relating to process assessment – First Edition
ISO 8000-120	Data quality – Part 120: Master data: Exchange of characteristic data: Provenance – First Edition
ISO 8000-63	Data quality Part 63: Data quality management: Process measurement
ISO/IEC 25020	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Quality measurement framework – Second edition
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
CEN 16991	Risk-based inspection framework – CORR: August 31, 2018
IEC 31010	Risk management – Risk assessment techniques

ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/IEC/IEEE 26511	Systems and software engineering – Requirements for managers of information for users of systems, software, and services
ISO/TS 8000-65	Data quality – Part 65: Data quality management: Process measurement questionnaire
ISO/TS 9002	Quality management systems – Guidelines for the application of ISO 9001:2015 – CORR: November 30, 2016
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO TS 8000-60	Data quality – Part 60: Data quality management: Overview – First Edition
ISO 8000-115	Data quality – Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolution requirements – First Edition
ISO/IEC TR 12382	Permuted Index of the Vocabulary of Information Technology – Second Edition
ISO 19115.1	Geographic information-Metadata Part 1: Fundamentals – Incorporating Amendment No. 1: June 2018
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO TR 14873	Information and documentation – Statistics and quality issues for web archiving – First Edition
ITU-T E.840	Statistical framework for end-to-end network performance benchmark scoring and ranking – Study Group 12

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
ISO 25000 series	SQuaRE (System and Software Quality Requirements and Evaluation)
ISO 25012	Software engineering – Software product Quality Requirements and Evaluation (SQuaRE) – Data quality model
ISO 8000 series	Data Quality and Enterprise Master Data
n/a	FAIR Principles
n/a	Statistics Canada's Quality Assurance Framework
n/a	Statistics Canada's Quality Assurance Framework
n/a	Statistics Canada's Data Quality Toolkit
IEEE P2896	Standard for Open Data: Open Data Ontology
IEEE P2957	Standard for a Reference Architecture for Big Data Governance and Metadata Management
IEEE P2963	Data Formats for Smart Legal Contracts
IEEE P2975	Standard for Industrial Artificial Intelligence (AI) Data Attributes
IEEE P3205	Standard for Blockchain Interoperability – Data Authentication and Communication Protocol
IEEE P3803	Standard for Household Appliance Customer Data Assetization and Commercialization Requirements

Working Group 3:
Data Access, Sharing, and Retention

Issue 19 —
Consent Management (Consent, Access and Withdrawal to Data)

BSI BS 10012	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 8611	Robots and robotic devices Guide to the ethical design and application of robots and robotic systems
BSI PAS 1192-5	Specification for security-minded building information modelling, digital built environments and smart asset management
BSI PD CEN/TS 16685	Information technology – Notification of RFID – The information sign to be displayed in areas where RFID interrogators are deployed
BSI PD CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
CEN EN 14484	Health informatics – International transfer of personal health data covered by the EU data protection directive – High level security policy; German version EN 14484:2003, text in English
CEN EN 14485	Health informatics – Guidance for handling personal health data in international applications in the context of the EU data protection directive
CEN EN 14822-2	Health informatics – General purpose information components – Part 2: Non-clinical; English version EN 14822-2:2005
CEN EN 15224	Quality management systems – EN ISO 9001:2015 for healthcare
CEN/TR 15300	Health Informatics – Framework for formal modelling of healthcare security policies
CEN/TR 16674	Information technology – Analysis of privacy impact assessment methodologies relevant to RFID
CEN/TS 15480-4	Identification card systems – European Citizen Card – Part 4: Recommendations for European Citizen Card issuance, operation and use
CEN-EN 16571	Information technology – RFID privacy impact assessment process
CLSI HS1-A2	A Quality Management System Model for Health Care; Approved Guideline – Second Edition; Vol 24; No 37
CLSI QMS01-A4	Quality Management System: A Model for Laboratory Services; Approved Guideline – Fourth Edition; Vol 31; No 15
CLSI QMS22	Management of Paper-based and Electronic Laboratory Information – First Edition
CSA CAN/CSA-C22.2 NO. 60950-23-07	Information Technology Equipment – Safety – Part 23: Large Data Storage Equipment – First Edition
CSA CAN/ CSA-Z900.2.1-17	Tissues for assisted reproduction – Third Edition
CSA CSA Z710:15	Métis Nation Registry Operations – First Edition
CSA CSA-Q830-03	Model Code for the Protection of Personal Information – Second Edition
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
CSA Z316.7-12	Primary sample collection facilities and medical laboratories – Patient safety and quality of care – Requirements for collecting, transporting, and storing samples – First Edition
CSA Z8000-18	Canadian health care facilities – Second Edition
DS DS/CWA 50487	SmartHouse Code of Practice
ETSI EG 202 487	Human Factors (HF); User experience guidelines; Telecare services (eHealth) – V1.1.2

ETSI GS INS 009	Identity and access management for Networks and Services (INS); Security and privacy requirements for collaborative cross domain network monitoring – V1.1.1
ETSI GS ISI 002	Information Security Indicators (ISI); Event Model A security event classification model and taxonomy – V1.2.1
ETSI GS ISI 005	Information Security Indicators (ISI); Guidelines for security event detection testing and assessment of detection effectiveness – V1.1.1
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach – V1.1.1
ETSI TR 102 688-8	Media Content Distribution (MCD); MCD framework; Part 8: Audience Measurement – V1.1.1
ETSI TR 102 935	Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform – V2.1.1
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TR 118 516	oneM2M; Study of Authorization Architecture for Supporting Heterogeneous Access Control Policies – V2.0.0; oneM2M TR-0016 version 2.0.0
IEEE 1735	Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP) – IEEE Computer Society; Incorporating Corrigendum 1: 2015
ISO 10781	Health Informatics – HL7 Electronic Health Records-System Functional Model, Release 2 (EHR FM)
ISO 22600-3	Health informatics – Privilege management and access control – Part 3: Implementations (ISO 22600-3:2014)
ISO 22857	Health informatics – Guidelines on data protection to facilitate transborder flows of personal health data
ISO 5127	Information and documentation – Foundation and vocabulary
ISO 8000-100	Data quality – Part 100: Master data: Exchange of characteristic data: Overview
ISO 8000-120	Data quality – Part 120: Master data: Exchange of characteristic data: Provenance
ISO 8000-130	Data quality – Part 130: Master data: Exchange of characteristic data: Accuracy
ISO 8000-140	Data quality – Part 140: Master data: Exchange of characteristic data: Completeness
ISO 8000-61	Data quality – Part 61: Data quality management: Process reference model – First Edition
ISO 834-2	Fire-resistance tests – Elements of building construction Part 2: Requirements and recommendations for measuring furnace exposure on test samples
ISO HL7 21731	Health informatics HL7 version 3 Reference information model Release 1 – First Edition; Corrected Version 10/15/2012
ISO TR 11636	Health Informatics – Dynamic on-demand virtual private network for health information infrastructure – First Edition
ISO TS 20658	Medical laboratories – Requirements for collection, transport, receipt, and handling of samples – First Edition
ISO TS 27790	Health informatics – Document registry framework – First Edition
ISO TS 29585	Health informatics – Deployment of a clinical data warehouse – First Edition
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition
ISO/IEC 10181-3	Information technology – Open Systems Interconnection – Security frameworks for open systems – Part 3: Access control framework
ISO/IEC 10746-2	Information technology – Open distributed processing – Reference model: Foundations
ISO/IEC 10779	Information technology – Office equipment – Accessibility guidelines for older persons and persons with disabilities
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services

ISO/IEC 24745	Information technology – Security techniques – Biometric information protection
ISO/IEC 29100	Information technology – Security techniques – Privacy framework – AMD: July 31, 2018
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment – CORR: April 30, 2020
ISO/IEC 29146	Information technology – Security techniques – A framework for access management
ISO/IEC 29187-1	Information technology – Identification of privacy protection requirements pertaining to learning, education and training (LET) – Part 1: Framework and reference model – First Edition
ISO/IEC TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commercial applications – Part 1: General guidance (Technical Report)
ISO/IEC TR 24729-4	Information technology – Radio frequency identification for item management – Implementation guidelines – Tag data security
ISO/IEC TR 24772	Information technology – Programming languages – Guidance to avoiding vulnerabilities in programming languages through language selection and use
ISO/TR 17791	Health informatics – Guidance on standards for enabling safety in health software
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 14265	Health informatics – Classification of purposes for processing personal health information – CORR: March 31, 2014
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – CORR: February 28, 2014
ISO/TS 19475-2	Document management – Minimum requirements for the storage of documents Part 2: Storage
ISO/TS 20658	Medical laboratories – Requirements for collection, transport, receipt, and handling of samples
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles
ISO/TS 22600-3	Health informatics – Privilege management and access control – Part 3: Implementations
ISO/TS 27790	Health informatics – Document registry framework
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ANSI AARST MS-QA	Radon Measurement Systems Quality Assurance
ISO/IEC 29190:18	Information technology – Security techniques – Privacy capability assessment model
ISO/IEC TR 23186:20	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

ISO/WD 24366	Natural Persons Identifier
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
IEEE P7002	Data Privacy Process
IEEE P7004	Standard for Child and Student Data Governance
IEEE P7005	IEEE Draft Standard for Transparent Employer Data Governance
IEEE P7006	Standard for Personal Data Artificial Intelligence (AI) Agent
IEEE P7008	Standard for Ethically Driven Nudging for Robotic, Intelligent and Autonomous Systems
IEEE P7012	Standard for Machine Readable Personal Privacy Terms
IEEE P7014	Standard for Ethical considerations in Emulated Empathy in Autonomous and Intelligent Systems

IEEE P2089	Standard for Age Appropriate Digital Services Framework – Based on the 5Rights Principles for Children
IEEE P3800	Standard for a data-trading system: overview, terminology and reference model
IEEE P2895	Standard Taxonomy for Responsible Trading of Human-Generated Data
IEEE IC16-002	The Global Initiative on Ethics of Autonomous and Intelligent Systems
IEEE IC17-002	Digital Inclusion, Identity, Trust, and Agency
IEEE IC19-004	Technology and Data Harmonization for Enabling Clinical Decentralized Clinical Trials
IEEE IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

Issue 20 — Data Access

BSI BS 10102-2	Big data Part 2: Guidance on data-intensive projects
ISO 23081-2	Information and documentation – Managing metadata for records – Part 2: Conceptual and implementation issues
ISO/IEC 13522-6	Information Technology – Coding of Multimedia and Hypermedia Information – Part 6: Support for Enhanced Interactive Applications
ISO/IEC 27002	Information technology – Security techniques – Code of practice for information security controls
ISO/IEC 27040	Information technology – Security techniques – Storage security (ISO/IEC 27040:2015)
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29146	Information technology – Security techniques – A framework for access management – First Edition
ISO/IEC TR 30166	Internet of Things (IoT) – Industrial IoT
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
IEEE P2975	Standard for Industrial Artificial Intelligence (AI) Data Attributes
CSA Z8003	Health care design research and evaluation

Issue 21 — Data retention

CEN EN 14484	Health informatics – International transfer of personal health data covered by the EU data protection directive – High level security policy; German version EN 14484:2003, text in English
ANSI INCITS 306	Information Technology – SCSI-3 Block Commands (SBC)
ANSI INCITS 516	Information Technology – SCSI Stream Commands – 4 (SSC-4)

ANSI X9.129	Legal Orders Exchange – Version 02
ANSI X9.84	Biometric Information Management and Security for the Financial Services Industry
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code of practice for implementation of BS 10008-1
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and information services
BSI PAS 1885	The fundamental principles of automotive cyber security – Specification
CEN EN 14485	Health informatics – Guidance for handling personal health data in international applications in the context of the EU data protection directive; German version EN 14485:2003, text in English
CEN EN 16072	Intelligent transport systems – ESafety – Pan-European eCall operating requirements
CEN EN 16571	Information technology – RFID privacy impact assessment process
CEN/TR 16673	Information technology – RFID privacy impact assessment analysis for specific sectors
CEN/TR 16674	Information technology – Analysis of privacy impact assessment methodologies relevant to RFID
CEN/TR 16742	Intelligent transport systems – Privacy aspects in ITS standards and systems in Europe
CEN/TS 15480-4	Identification card systems – European Citizen Card – Part 4: Recommendations for European Citizen Card issuance, operation and use
CENELEC CEN/CLC/ ETSI/TR 50572	Functional reference architecture for communications in smart metering systems
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
DS DS/CWA 17356	Interoperability of security systems for the surveillance of widezones
ETSI EG 202 798	Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing – V1.1.1
ETSI ETR 295	Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); User Requirements for Subscriber Identity Module (SIM)
ETSI GS INS 009	Identity and access management for Networks and Services (INS); Security and privacy requirements for collaborative cross domain network monitoring – V1.1.1
ETSI GS ISI 008	Information Security Indicators (ISI); Description of an Overall Organization-wide Security Information and Event Management (SIEM) Approach – V1.1.1
ETSI GS MOI 002	Measurement Ontology for IP traffic (MOI); Requirements for IP traffic measurement ontologies development – V1.1.1
ETSI GS MOI 003	Measurement Ontology for IP traffic (MOI); IP traffic measurement ontologies architecture – V1.1.1; Includes Diskette
ETSI GS MOI 010	Measurement Ontology for IP traffic (MOI); Report on information models for IP traffic measurement – V1.1.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns – V1.1.1
ETSI GS NGP 001	Next Generation Protocols (NGP); Scenario Definitions – V1.3.1
ETSI SR 002 298	Response from CEN and ETSI to the “Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for a European Policy Approach” – V1.1.1
ETSI SR 002 564	Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth – V2.0.0
ETSI SR 003 392	Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards – V2.1.1

ETSI TR 102 299	Emergency Communications (EMTEL); Collection of European Regulatory Texts and orientations – V1.4.1
ETSI TR 102 438	Electronic Signatures and Infrastructures (ESI); Application of Electronic Signature Standards in Europe – V1.1.1
ETSI TR 102 512	Terrestrial Trunked Radio (TETRA); Security; Security requirements analysis for modulation enhancements to TETRA
ETSI TR 102 725	Machine-to-Machine communications (M2M); Definitions – V1.1.1
ETSI TR 102 762	Human Factors (HF); Intelligent Transport Systems (ITS); ICT in cars – V1.1.1
ETSI TR 103 118	Machine-to-Machine communications (M2M); Smart Energy Infrastructures security; Review of existing security measures and convergence investigations – V1.1.1
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 533	SmartM2M; Security; Standards Landscape and best practices – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TS 102 412	Smart Cards; Smart Card Platform Requirements Stage 1 – V12.1.0; Release 12
ETSI TS 102 657	Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data – V1.25.1; Includes Diskette
ETSI TS 103 443-2	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 2: NAT64 – V1.1.1
ETSI TS 103 443-3	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 3: DS-Lite – V1.1.1
ETSI TS 103 443-5	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 5: 464XLAT – V1.1.1
ETSI TS 103 443-6	Integrated broadband cable telecommunication networks (CABLE); IPv6 Transition Technology Engineering and Operational Aspects; Part 6: 6RD – V1.1.1
ETSI TS 105 174-2	Access, Terminals, Transmission and Multiplexing (ATTM); Broadband Deployment and Lifecycle Resource Management; Part 2: ICT Sites: Implementation of energy and lifecycle management practices – V1.3.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
IEC 61360-4	Standard data element types with associated classification scheme for electric components – Part 4: IEC reference collection of standard data element types and component classes
IEC 61512-4	Batch control Part 4: Batch production records
IEC 63119-1	Information exchange for electric vehicle charging roaming service Part 1: General
IEC 82304-1	Health Software – Part 1: General requirements for product safety
IEC TR 80001-2-8	Application of risk management for IT-networks incorporating medical devices – Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
IEC/TR 62939-1	Smart grid user interface Part 1: Interface overview and country perspectives
IEC/TR 80001-2-8	Application of risk management for IT-networks incorporating medical devices Part 2-8: Application guidance – Guidance on standards for establishing the security capabilities identified in IEC TR 80001-2-2
IEEE 2001	Recommended Practice for the InternetWeb Site Engineering, Web Site Management, and Web Site Life Cycle – IEEE Computer Society Document
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society

IEEE 2755.1	Guide for Taxonomy for Intelligent Process Automation Product Features and Functionality
ISO/IEC 15944-9	Information technology – Business Operational View – Part 9: Business transaction traceability framework for commitment exchange
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ISO/IEC 17789:16	Information technology – Cloud computing – Reference architecture
ISO/IEC 18014-4	Information technology – Security techniques – Time-stamping services Part 4: Traceability of time sources
ISO/IEC 18043	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems
ISO/IEC 19086-1	Information technology – Cloud computing – Service level agreement (SLA) framework Part 1: Overview and concepts
ISO/IEC 19086-3	Information technology – Cloud computing – Service level agreement (SLA) framework Part 3: Core conformance requirements
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use
ISO/IEC 20748.2	Information technology for learning, education and training – Learning analytics interoperability Part 2: System requirements
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 27004	Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation
ISO/IEC 27034-5	Information technology – Security techniques – Application security Part 5: Protocols and application security controls data structure
ISO/IEC 27037	Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012)
ISO/IEC 27039	Information technology – Security techniques – Selection, deployment and operations of intrusion detection systems (IDPS) – CORR: June 30, 2018
ISO/IEC 27040	Information technology – Security techniques – Storage security
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29100	Information technology – Security techniques – Privacy framework – AMD: July 31, 2018
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29110-4-3	Systems and software engineering – Lifecycle profiles for very small entities (VSEs) – Part 4-3: Service delivery – Profile specification – First Edition
ISO/IEC 29134	Information technology – Security techniques – Guidelines for privacy impact assessment – First Edition
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiable information protection
ISO/IEC 29155-2	Systems and software engineering – Information technology project performance benchmarking framework Part 2: Requirements for benchmarking
ISO/IEC 29184	Information technology – Online privacy notices and consent
ISO/IEC 29341-30-1	Information technology – UPnP Device Architecture – Part 30-1: IoT management and control device control protocol – IoT management and control architecture overview – First Edition

ISO/IEC 30137-1	Information technology – Use of biometrics in video surveillance systems Part 1: System design and specification
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data
ISO/IEC TR 15067-3-2	Information technology – Home electronic system application model Part 3-2: GridWise – Interoperability context-setting framework
ISO/IEC TR 15947	Information technology – Security techniques – IT intrusion detection framework
ISO/IEC TR 16166	Information technology – Telecommunications and information exchange between systems – Next Generation Corporate Networks (NGCN) – Security of session-based communications – First Edition
ISO/IEC TR 20000-9	Information technology – Service management Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services
ISO/IEC TR 20748-2	Information technology for learning, education and training – Learning analytics interoperability Part 2: System requirements – CORR: August 31, 2018
ISO/IEC TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commerical applications Part 1: General guidance
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 29110-5-3	Systems and software engineering – Lifecycle profiles for Very Small Entities (VSEs) Part 5-3: Service delivery guidelines
ISO/IEC TR 29196	Information technology – Guidance for biometric enrolment
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TS 27034-5-1	Information technology – Application security – Part 5-1: Protocols and application security controls data structure, XML schemas
ISO/IEC/IEEE 12207	Systems and software engineering – Software life cycle processes
ISO/IEC/IEEE 15289	Systems and software engineering – Content of life-cycle information items (documentation)
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems, software, and services information
ISO/IEC/IEEE 24765	Systems and software engineering – Vocabulary
ISO/IEC/IEEE 29148	Systems and software engineering – Life cycle processes – Requirements engineering
ISO/IEC/IEEE 90003	Software engineering – Guidelines for the application of ISO 9001:2015 to computer software
ISO/TR 10255	Document management applications – Optical disk storage technology, management and standards
ISO/TR 12859	Intelligent transport systems – System architecture – Privacy aspects in ITS standards and systems
ISO/TR 14742	Financial services – Recommendations on cryptographic algorithms and their use
ISO/TR 17427-3	Intelligent transport systems – Cooperative ITS Part 3: Concept of operations (ConOps) for 'core' systems
ISO/TR 17427-4	Intelligent transport systems – Cooperative ITS Part 4: Minimum system requirements and behaviour for core systems
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/TR 17797	Electronic archiving – Selection of digital storage media for long term preservation
ISO/TR 80002-2	Medical device software Part 2: Validation of software for medical device quality systems
ISO/TS 17427	Intelligent transport systems – Cooperative systems – Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems (ISO/TS 17427:2014); English version CEN ISO/TS 17427:2014
ISO/TS 19299	Electronic fee collection – Security framework (ISO/TS 19299:2015); English version CEN ISO/TS 19299:2015

ISO/TS 21089	Health informatics – Trusted end-to-end information flows
ISO/TS 26683-1	Intelligent transport systems – Freight land conveyance content identification and communication (FLC-CIC) – Part 1: Context, architecture and referenced standards
ITU-T L.1300	Best practices for green data centres – Study Group 5
ITU-T L.64	ID tag requirements for infrastructure and network elements management – Study Group 15
ITU-T M.3363	Requirements for data management in the telecommunication management network – Study Group 2
ITU-T SERIES D SUPP 4	Principles for increased adoption and use of mobile financial services (MFSs) through effective consumer protection mechanisms – Study Group 3
ITU-T SERIES X SUPP 13	ITU-T X.1051 – Supplement on information security management users' guide for Recommendation ITU-T X.1051 – Study Group 17
ITU-T SERIES X SUPP 32	ITU-T X.1058 – Supplement on code of practice for personally identifiable information (PII) protection for telecommunications organizations – Study Group 17
ITU-T SERIES Y SUPP 40	Big data standardization roadmap – Study Group 13
ITU-T SERIES Y SUPP 55	ITU-T Y.3170-series – Machine learning in future networks including IMT-2020: Use cases – Study Group 13
ITU-T X.1058	Information technology – Security techniques – Code of practice for personally identifiable information protection – Study Group 17
ITU-T X.1147	Security requirements and framework for big data analytics in mobile Internet services – Study Group 17
ITU-T X.1250	Baseline capabilities for enhanced global identity management and interoperability – Study Group 17
ITU-T X.1601	Security framework for cloud computing – Study Group 17
ITU-T X.1602	Security requirements for software as a service application environments – Study Group 17
ITU-T X.1603	Data security requirements for the monitoring service of cloud computing – Study Group 17
ITU-T X.1642	Guidelines for the operational security of cloud computing – Study Group 17
ITU-T Y.3174	Framework for data handling to enable machine learning in future networks including IMT-2020 – Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ITU-T Y.3604	Big data – Overview and requirements for data preservation – Study Group 13
ITU-T Y.4556	Requirements and functional architecture of smart residential community – Study Group 20

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 104	Baseline Cyber Security Controls for Small and Medium Organizations
IEEE 1619-2018	IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices –

Issue 22 —
Identity management – validation and authentication (People, Entity & Devices)

ANSI INCITS 501	Information Technology – Security Features for SCSI Commands (SFSC)
ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ANSI X9 TR-48	Card-Not-Present (CNP) Fraud Mitigation in the United States: Strategies for Preventing, Detecting, and Responding to a Growing Threat – ASCX9
ANSI X9.111	Penetration Testing within the Financial Services Industry – ASCX9
ANSI X9.73	Cryptographic Message Syntax – ASN.1 and XML – ASCX9
ANSI X9.84	Biometric Information Management and Security for the Financial Services Industry
BSI PAS 11281	Connected automotive ecosystems – Impact of security on safety – Code of practice
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
BSI PAS 499	Code of practice for digital identification and strong customer authentication
BSI PAS 96	Guide to protecting and defending food and drink from deliberate attack
CEN 12830	Temperature recorders for the transport, storage and distribution of temperature sensitive goods – Tests, performance, suitability
CEN 16495	Air Traffic Management – Information security for organisations supporting civil aviation operations
CEN 419221-5	Protection Profiles for TSP Cryptographic Modules Part 5: Cryptographic Module for Trust Services
CEN EN 12896-5	Public transport – Reference data model – Part 5: Fare management
CEN/TS 16614-3	Public transport – Network and Timetable Exchange (NeTEx) Part 3: Public transport fares exchange format
DS DS/CWA 17302	City Resilience Development – Information Portal
DIN CEN/TS 16614-3	Public transport – Network and Timetable Exchange (NeTEx) – Part 3: Public transport fares exchange format; English version CEN/TS 16614-3:2016, only on CD-ROM
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91347	Integrated multi-functional Humble Lamppost (imHLa)
ETSI EN 319 411-1	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements – V1.2.2
ETSI EN 319 521	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Electronic Registered Delivery Service Providers – V1.1.1
ETSI EN 319 522-2	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 2: Semantic contents – V1.1.1
ETSI EN 319 522-3	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 3: Formats – V1.1.1; Includes Diskette
ETSI EN 319 522-4-3	Electronic Signatures and Infrastructures (ESI); Electronic Registered Delivery Services; Part 4: Bindings; Sub-part 3: Capability/requirements bindings – V1.1.1
ETSI EN 319 532-3 V1.2.1	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 3: Formats
ETSI GR PDL 001	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies – V1.1.1
ETSI GS ISI 002	Information Security Indicators (ISI); Event Model A security event classification model and taxonomy – V1.2.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns – V1.1.1
ETSI GS NFV-SEC 014	Network Functions Virtualisation (NFV) Release 3; NFV Security; Security Specification for MANO Components and Reference points – V3.1.1

ETSI SR 003 186	Electronic Signatures and Infrastructures (ESI) Testing interoperability and conformity activities to be run during the implementation and promotion of the framework of digital signatures – V2.1.1
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI SR 019 050	Electronic Signatures and Infrastructures (ESI); Rationalized framework of Standards for Electronic Registered Delivery Services Applying Electronic Signatures – V1.1.1; Includes Diskette
ETSI TR 103 303	CYBER; Protection measures for ICT in the context of Critical Infrastructure – V1.1.1
ETSI TR 103 305-1	CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls – V3.1.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 604	User Group; User centric approach; Qualification of the interaction with the digital ecosystem – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TR 103 684	Electronic Signatures and Infrastructures (ESI); Global Acceptance of EU Trust Services – V1.1.1
ETSI TR 119 530	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Feasibility study: Interoperability profile between ETSI EN 319 532-based REM systems and PReM-based systems – V1.1.1
ETSI TS 133 501	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.4.0 Release 16)
ETSI TS 101 553-2	Core Network and Interoperability Testing (INT); Testing of the IBCF requirements; (3GPP Release 12); Part 2: Test Suite Structure and Test Purposes (TSS&TP) – V4.1.1
ETSI TS 102 412	Smart Cards; Smart Card Platform Requirements Stage 1 – V12.1.0; Release 12
ETSI TS 103 436	Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios – V1.2.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 645	CYBER; Cyber Security for Consumer Internet of Things – V1.1.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
ETSI TS 119 102-2	Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 2: Signature Validation Report – V1.2.1; Includes Diskette
ETSI TS 119 403-3	Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 3: Additional requirements for conformity assessment bodies assessing EU qualified trust service providers – V1.1.1
ETSI TS 119 432	Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation – V1.1.1; Includes Diskette
ETSI TS 119 512	Electronic Signatures and Infrastructures (ESI); Protocols for trust service providers providing long-term data preservation services – V1.1.1
ETSI TS 119 524-1	Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Electronic Registered Delivery Services; Part 1: Testing conformance – V1.1.1
ETSI TS 119 534-1	Electronic Signatures and Infrastructures (ESI); Testing Conformance and Interoperability of Registered Electronic Mail Services; Part 1: Testing conformance – V1.1.1
ETSI TS 119 612	Electronic Signatures and Infrastructures (ESI); Trusted Lists – V2.2.1; Includes Diskette
ETSI TS 133 107	Universal Mobile Telecommunications System (UMTS); LTE; Digital cellular telecommunications system (Phase 2+) (GSM); 3G security; Lawful interception architecture and functions – V15.6.0; 3GPP TS 33.107 version 15.6.0 Release 15
ETSI TS 133 180	LTE; Security of the mission critical service – V15.7.0; 3GPP TS 33.180 version 15.7.0 Release 15
ETSI TS 133 401	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture – V15.11.0; 3GPP TS 33.401 version 15.11.0 Release 15
IEC 60050-741	International Electrotechnical Vocabulary (IEV) – Part 741: Internet of Things (IoT) – Edition 1.0
IEC 60839-5-3	Alarm and electronic security systems – Part 5-3: Alarm transmission systems – Requirements for receiving centre transceiver (RCT)

IEC 62443-2-4	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers
IEC TR 62559-1	Use case methodology Part 1: Concept and processes in standardization
IEEE 1865	Maintenance and Test of Distributed Control Systems in Thermal Power Stations: General Requirements and Definitions
IEEE 1865.2	Standard Specifications for Maintenance and Test of Distributed Control Systems in Thermal Power Stations: Operation Service and Management
IEEE 1934	Adoption of OpenFog Reference Architecture for Fog Computing
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 802.1CF	Recommended Practice for Network Reference Model and Functional Description of IEEE 802® Access Network – IEEE Computer Society
IEEE 802.1X	Local and Metropolitan Area Networks – Port-Based Network Access Control – IEEE Computer Society; Includes Access to Additional Content
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	PHD Cybersecurity Standards Roadmap – Version: 1.0
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 12812-1	Core banking – Mobile financial services Part 1: General framework
ISO 14721	Space data and information transfer systems – Open archival information system (OAIS) – Reference model
ISO 15118-1	Road vehicles – Vehicle to grid communication interface Part 1: General information and use-case definition
ISO 16484-5	Building automation and control systems (BACS) – Part 5: Data communication protocol (ISO 16484-5:2017)
ISO 20700	Guidelines for management consultancy services
ISO 22300	Security and resilience – Vocabulary (ISO 22300:2018)
ISO 9564-4	Financial services – Personal Identification Number (PIN) management and security – Part 4: Requirements for PIN handling in eCommerce for Payment Transactions
ISO TS 11633-1	Health informatics – Information security management for remote maintenance of medical devices and medical information systems – Part 1: Requirements and risk analysis – First edition
ISO TS 12812-5	Core Banking – Mobile Financial Services – Part 5: Mobile Payments to Business – First Edition
ISO TS 23029	Web-service-based application programming interface (WAPI) in financial services – First edition
ISO/IEC 14776-454	Information technology – Small Computer System Interface (SCSI) – Part 454: SCSI Primary Commands – 4 (SPC-4)
ISO/IEC 14776-481	Information technology – Small computer system interface (SCSI) – Part 481: Part 481: Security Features for SCSI Commands (SFSC)
ISO/IEC 18013-1	Information technology – Personal identification – ISO-compliant driving licence – Part 1: Physical characteristics and basic data set
ISO/IEC 18028-4	Information technology – Security techniques – IT network security – Part 4: Securing remote access
ISO/IEC 18370-2	Information technology – Security techniques – Blind digital signatures – Part 2: Discrete logarithm based mechanisms
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – First Edition

ISO/IEC 20248	Information technology – Automatic identification and data capture techniques – Data structures – Digital signature meta structure – First Edition
ISO/IEC 20924	Internet of things (IoT) – Vocabulary
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation of virtualized servers
ISO/IEC 23006-3	Information technology – Multimedia service platform technologies – Part 3: Conformance and reference software – Third Edition
ISO/IEC 24759	Information technology – Security techniques – Test requirements for cryptographic modules – Third Edition
ISO/IEC 24760-1	IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management – Part 3: Practice
ISO/IEC 25023	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality
ISO/IEC 27019	Information technology – Security techniques – Information security controls for the energy utility industry
ISO/IEC 27021	Information technology – Security techniques – Competence requirements for information security management systems professionals – First Edition
ISO/IEC 27036-4	Information technology – Security techniques – Information security for supplier relationships Part 4: Guidelines for security of cloud services
ISO/IEC 30107-1	Information technology – Biometric presentation attack detection Part 1: Framework
ISO/IEC 30118-2	Information technology – Open Connectivity Foundation (OCF) Specification – Part 2: Security specification
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derived requirements – First Edition
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC TR 29156	Information technology – Guidance for specifying performance requirements to meet security and usability needs in applications using biometrics
ISO/IEC TR 30125	Information technology – Biometrics used with mobile devices
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operational environment
ISO/IEC TS 27008	Information technology – Security techniques – Guidelines for the assessment of information security controls
ISO/IEC/IEEE 8802-21	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 21: Media independent services framework
ISO/IEC/IEEE 8802-21-1	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Part 21-1: Media independent services
ISO/TR 20526	Account-based ticketing state of the art report
ISO/TS 11633-1	Health informatics – Information security management for remote maintenance of medical devices and medical information systems Part 1: Requirements and risk analysis
ISO/TS 12812-5	Core banking – Mobile financial services Part 5: Mobile payments to businesses
ISO/TS 23029	Web-service-based application programming interface (WAPI) in financial services
ITU-T G.7701	Common control aspects – Study Group 15
ITU-T H.550	Architecture and functional entities of vehicle gateway platforms – Study Group 16
ITU-T J.1	(Pre-Published) Terms, definitions and acronyms for television and sound transmission and integrated broadband cable networks

ITU-T J.298	Requirements and technical specifications of a cable TV hybrid set-top box compatible with terrestrial and satellite TV transport – Study Group 9
ITU-T P.1502	Methodology for QoE testing of digital financial services – Study Group 12
ITU-T SERIES F SUPP 3	Overview of Telecom Finance (Finance 2.0) – Study Group 2
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T SERIES Y SUPP 53	ITU-T Y.4000-series – Internet of Things use cases – Study Group 20
ITU-T SERIES Y SUPP 56	ITU-T Y-series – Supplement on use cases of smart cities and communities – Study Group 20
ITU-T X.1038	Security requirements and reference architecture for software-defined networking – Study Group 17
ITU-T X.1039	Technical security measures for implementation of ITU-T X.805 security dimensions – Study Group 17
ITU-T X.1087	Technical and operational countermeasures for telebiometric applications using mobile devices – Study Group 17
ITU-T X.1127	Functional security requirements and architecture for mobile phone anti-theft measures – Study Group 17
ITU-T X.1146	(Pre-Published) Secure protection guidelines for value-added services provided by telecommunication operators
ITU-T X.1258	Enhanced entity authentication based on aggregated attributes – Study Group 17
ITU-T X.1276	Authentication step-up protocol and metadata Version 1.0 – Study Group 17
ITU-T X.1277	Universal authentication framework – Study Group 17
ITU-T X.1331	Security guidelines for home area network (HAN) devices in smart grid systems – Study Group 17
ITU-T X.1450	Guidelines on hybrid authentication and key management mechanisms in the client-server model – Study Group 17
ITU-T X.1605	Security requirements of public Infrastructure as a Service (IaaS) in cloud computing – Study Group 17
ITU-T X.1631	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services – Study Group 17
ITU-T X.1642	Guidelines for the operational security of cloud computing – Study Group 17
ITU-T Y.2342	Scenarios and capability requirements of blockchain in next generation network evolution – Study Group 13
ITU-T Y.4459	Digital entity architecture framework for Internet of things interoperability – Study Group 20
SAE J3101	Hardware Protected Security for Ground Vehicles
SAE PT-179	Commercial Aviation Cyber Security: Current State and Essential Reading – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SNZ AS/NZS 62676.1.1	Video surveillance systems for use in security applications Part 1.1: System requirements – General
UL 827 BULLETIN	UL Standard for Safety Central-Station Alarm Services – COMMENTS DUE: June 22, 2020
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
ISO 17442:2019	Financial services – Legal entity identifier (LEI)
ISO/CD 24366	Natural Persons Identifier
CAN/CIOSC 103-1	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
Pan-Canadian Trust Framework	A collaborative approach to developing a Pan-Canadian Trust Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals

CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 103-3	Digital trust and identity – Part 3: Digital credentials
CAN/CIOSC 103-4	Digital trust and identity – Part 4: Digital wallets
IEEE P1363.3/D9	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings
IEEE 802.1AR-2018	IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity
IEEE 2410-2019	IEEE Standard for Biometric Open Protocol
DIACC PCTF 01	Pan-Canadian Trust Framework (PCTF) Model v1.0
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent: Component Overview and Conformance Profile v1.0
DIACC PCTF 03	Pan-Canadian Trust Framework (PCTF) Authentication: Component Overview and Conformance Profile v1.0
DIACC PCTF 04	Pan-Canadian Trust Framework (PCTF) Privacy: Component Overview and Conformance Profile v1.0
DIACC PCTF 05	Pan-Canadian Trust Framework (PCTF) Verified Person: Component Overview and Conformance Profile v1.0
DIACC PCTF 06	Pan-Canadian Trust Framework (PCTF) Verified Organization: Component Overview and Conformance Profile v1.0
DIACC PCTF 07	Pan-Canadian Trust Framework (PCTF) Credentials (Relationship & Attributes): Component Overview and Conformance Profile v1.0
DIACC PCTF 08	Pan-Canadian Trust Framework (PCTF) Infrastructure (Technology & Operations): Component Overview and Conformance Profile v1.0
DIACC PCTF 09	Pan-Canadian Trust Framework (PCTF) Assessment v1.0
DIACC PCTF 10	Pan-Canadian Trust Framework (PCTF) Glossary V1.0

Issue 23 —
Data Sharing, Exchanging, and Integration

ISO/IEC TR 29144	Information technology – Biometrics – The use of biometric technology in commercial Identity Management applications and processes
CEN EN 16570	Information technology – Notification of RFID – The information sign and additional information to be provided by operators of RFID application systems
ISO 20614	Information and documentation – Data exchange protocol for interoperability and preservation
DIN 66398	Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information
ANSI INCITS 459	Information Technology – Requirements for the Implementation and Interoperability of Role Based Access Control
ANSI INCITS 398	Information Technology Common Biometric Exchange Formats Framework (CBEFF)
ASTM E2468	Standard Practice for Metadata to Support Archived Data Management Systems
ISO/IEC 24713-3	Information technology – Biometric profiles for interoperability and data exchange Part 3: Biometrics-based verification and identification of seafarers
NFPA 951	Guide to Building and Utilizing Digital Information – Effective date: 4/12/2015
ISO/IEC 18598	Information technology – Automated infrastructure management (AIM) systems – Requirements, data exchange and applications
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management

ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC TS 27008	Information technology – Security techniques – Guidelines for the assessment of information security controls
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 100-9	Data Governance – Part 9: Zero Copy Integration
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
CAN/CIOSC 106-1	Discovery and management of Digital Twins for built environments – Part 1: Discovery
CAN/CIOSC 106-2	Discovery and management of Digital Twins for built environments – Part 2: Management
CAN/CIOSC 109-2	Canadian Information Privacy Protection Framework
IEEE/IEC 61671-2-2016	IEC/IEEE International Standard for Automatic Test Markup Language (ATML) Instrument Description
IEEE 1671.2	IEEE Trial-Use Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic Test Equipment and Test Information via XML: Exchanging Instrument Descriptions
IEEE 1671.3	IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic Test Information via XML (eXtensible Markup Language): Exchanging UUT (Unit Under Test) Description Information
IEEE 1671.4	IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic Test Information via eXtensible Markup Language (XML): Exchanging Test Configuration Information
IEEE 1671.5	IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic Test Information via XML:Exchanging Test Adapter Information
IEEE 1671.6	IEEE Standard for Automatic Test Markup Language (ATML) for Exchanging Automatic Test Information via XML: Exchanging Test Station Information
ISO/IEC/IEEE 18881:2016	ISO/IEC/IEEE Information technology- Ubiquitous green community control network protocol
IEEE P802.11bb	IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
CSA Z8003	Health care design research and evaluation

Issue 24 — Trusted Data Intermediaries

ETSI TS 133 501	5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.4.0 Release 16)
ISO TR 20526	Account-based ticketing state of the art report – First Edition
ISO TS 8000-150	Data quality – Part 150: Master data: Quality management framework – First Edition

ISO/IEC 15944-12	Information technology – Business operational view Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)
ISO/IEC 17788	Information technology – Cloud computing – Overview and vocabulary
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture (ISO/IEC 17789:2014)
ISO/IEC 17826	Information technology – Cloud Data Management Interface (CDMI)
ISO/IEC 19086-1	Information technology – Cloud computing – Service level agreement (SLA) framework – Part 1: Overview and concepts (ISO/IEC 19086-1:2016)
ISO/IEC 19086-4	Cloud computing – Service level agreement (SLA) framework – Part 4: Components of security and of protection of PII
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability – First Edition
ISO/IEC 21878	Information technology – Security techniques – Security guidelines for design and implementation of virtualized servers
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management – Part 3: Practice
ISO/IEC 27000	Information technology – Security techniques – Information security management systems – Overview and vocabulary
ISO/IEC 27009	Information technology – Security techniques – Sector-specific application of ISO/IEC 27001 – Requirements (ISO/IEC 27009:2016)
ISO/IEC 27018	Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
ISO/IEC 27036-4	Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services
ISO/IEC 27701	Expert commentary BS ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC 30141	Internet of Things (IoT) – Reference architecture
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data – First Edition
ISO/IEC TR 20000-9	Information technology – Service management Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services
ISO/IEC TR 20547-2	Information technology – Big data reference architecture – Part 2: Use cases and derived requirements – First Edition
ISO/IEC TR 22678	Information technology – Cloud computing – Guidance for policy development
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC TR 23187	Information technology – Cloud computing – Interacting with cloud service partners (CSNs) – First edition
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape – First edition
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing – First Edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/IEC TS 23167	Information technology – Cloud computing – Common technologies and techniques – First edition
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
n/a	Exploring Data Trust Certifications

CAN/CIOSC 103-1	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
Pan-Canadian Trust Framework	A collaborative approach to developing a Pan-Canadian Trust Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship

Issue 25 —
Authorization for data collection and sharing

ANSI INCITS 172	Information Technology – American National Standard Dictionary of Information Technology (ANSDIT)
ASHRAE 135	BACnet – A Data Communication Protocol for Building Automation and Control Networks
ASHRAE 201	Facility Smart Grid Information Model
ASTM E1578	Standard Guide for Laboratory Informatics
AWWA G410	Business Practices for Operation and Management
BSI BS 10012	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI PAS 1085	Manufacturing – Establishing and implementing a security-minded approach – Specification
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
BSI PAS 180	Smart cities – Vocabulary
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and information services
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach – CORR: May 30, 2018
CEN EN 14484	Health informatics – International transfer of personal health data covered by the EU data protection directive – High level security policy
CEN EN 14485	Health informatics – Guidance for handling personal health data in international applications in the context of the EU data protection directive; German version EN 14485:2003, text in English
CEN/TS 17470	Service model for social care alarms
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
DS DS/CWA 17145-1	Ethics assessment for research and innovation – Part 1: Ethics committee
ETSI GS INS 009	Identity and access management for Networks and Services (INS); Security and privacy requirements for collaborative cross domain network monitoring – V1.1.1
ETSI GS MOI 002	Measurement Ontology for IP traffic (MOI); Requirements for IP traffic measurement ontologies development – V1.1.1
ETSI SR 002 564	Applicability of existing ETSI and ETSI/3GPP deliverables to eHealth – V2.0.0

ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI TR 102 202	Human Factors (HF); Human Factors of work in call centres – V1.1.2
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 305	CYBER; Critical Security Controls for Effective Cyber Defence – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
ETSI TS 129 240	Universal Mobile Telecommunications System (UMTS); LTE; 3GPP Generic User Profile (GUP); Stage 3; Network – V15.0.0; 3GPP TS 29.240 version 15.0.0 Release 15
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 26514	Adoption of ISO/IEC 26514:2008 Systems and Software Engineering – Requirements for Designers and Developers of User Documentation – IEEE Computer Society
IEEE WHITE PAPER 3DBP IC	IEEE 3D BODY PROCESSING INDUSTRY CONNECTIONS (3DBP IC): COMMUNICATION, SECURITY, AND PRIVACY
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 13606-4	Health informatics – Electronic health record communication – Part 4: Security
ISO 18308	Health informatics – Requirements for an electronic health record architecture
ISO 19115-1	Geographic information – Metadata – Part 1: Fundamentals
ISO 19650-5	Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 5: Security-minded approach to information management – First edition
ISO 20252	Market, opinion and social research, including insights and data analytics – Vocabulary and service requirements
ISO 22857	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health data – Second Edition
ISO 24100	Intelligent transport systems – Basic principles for personal data protection in probe vehicle information services
ISO 24978	Intelligent transport systems – ITS Safety and emergency messages using any available wireless media – Data registry procedures (ISO 24978:2009); English version EN ISO 24978:2009
ISO 25237	Health informatics – Pseudonymization (ISO 25237:2017)
ISO 26000	Guidance on social responsibility (ISO 26000:2010)
ISO 29134	Information technology – Security techniques – Guidelines for privacy impact assessment (ISO/IEC 29134:2017)
ISO 35001	Biorisk management for laboratories and other related organisations – First edition
ISO 37156	Smart community infrastructures – Guidelines on data exchange and sharing for smart community infrastructures
ISO TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap – Part 2: Architectural components and maturity model – First Edition
ISO TR 17427-3	Intelligent transport systems – Cooperative ITS – Part 3: Concept of operations (ConOps) for 'core' systems – First Edition
ISO TR 17427-7	Intelligent transport systems – Cooperative ITS – Part 7: Privacy aspects – First Edition
ISO TR 22221	Health informatics Good principles and practices for a clinical data warehouse – First Edition
ISO TR 22758	Biotechnology – Biobanking – Implementation guide for ISO 20387 – First edition
ISO TS 12812-5	Core Banking – Mobile Financial Services – Part 5: Mobile Payments to Business – First Edition

ISO TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – First Edition
ISO TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information – First Edition
ISO TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care – First Edition
ISO TS 21089	Health informatics – Trusted end-toend information flows – First Edition
ISO TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles – First Edition
ISO TS 22220	Health informatics – Identification of subjects of health care – Second Edition
ISO TS 29585	Health informatics – Deployment of a clinical data warehouse – First Edition
ISO TS 37107	Sustainable cities and communities – Maturity model for smart sustainable communities – First edition
ISO/IEC 15504-6	Information technology – Process assessment – Part 6: An exemplar system life cycle process assessment model – First Edition
ISO/IEC 15944-9	Information technology – Business Operational View – Part 9: Business transaction traceability framework for commitment exchange
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ISO/IEC 18028-1	Information technology – Security techniques – IT network security Part 1: Network security management
ISO/IEC 18384-2	Information technology – Reference Architecture for Service Oriented Architecture (SOA RA) Part 2: Reference Architecture for SOA Solutions
ISO/IEC 19790	Information technology – Security techniques – Security requirements for cryptographic modules – Second Edition; Corrected version 12/15/2015
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability – First Edition
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use
ISO/IEC 20748.1	Information technology for learning, education and training – Learning analytics interoperability Part 1: Reference model
ISO/IEC 20748.2	Information technology for learning, education and training – Learning analytics interoperability Part 2: System requirements
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC 20944-1	Information technology – Metadata Registries Interoperability and Bindings (MDR-IB) Part 1: Framework, common vocabulary, and common provisions for conformance
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services
ISO/IEC 23092-1	Information technology – Genomic information representation – Part 1: Transport and storage of genomic information
ISO/IEC 23092-2	Information technology – Genomic information representation – Part 2: Coding of genomic information – First edition
ISO/IEC 23092-3	Information technology – Genomic information representation – Part 3: Metadata and application programming interfaces (APIs) – First edition
ISO/IEC 24760-1	Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts
ISO/IEC 24760-2	Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements – First Edition
ISO/IEC 24760-3	Information technology – Security techniques – A framework for identity management – Part 3: Practice
ISO/IEC 27033-1	Information technology – Security techniques – Network security – Part 1: Overview and concepts

ISO/IEC 27701	Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC 29155-4	Systems and software engineering – Information technology project performance benchmarking framework Part 4: Guidance for data collection and maintenance
ISO/IEC 30141	Internet of Things (IoT) – Reference Architecture
ISO/IEC/IEEE 12207	Systems and software engineering – Software life cycle processes
ISO/IEC/IEEE 15288	Systems and software engineering – System life cycle processes – First Edition
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems, software, and services information
ISO/IEC/IEEE 24748-1	Systems and software engineering – Life cycle management Part 1: Guidelines for life cycle management
ISO/IEC/IEEE 29148	Systems and software engineering – Life cycle processes – Requirements engineering
ISO/IEC/TR 13335-4	Information Technology – Guidelines for the Management of IT Security – Part 4: Selection of Safeguards (TECHNICAL REPORT)
ISO/IEC/TR 20748-1	Information technology for learning, education and training – Learning analytics interoperability Part 1: Reference model
ISO/IEC/TR 20748-2	Information technology for learning, education and training – Learning analytics interoperability Part 2: System requirements – CORR: August 31, 2018
ISO/IEC/TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC/TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC/TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commerical applications Part 1: General guidance
ISO/IEC/TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC/TR 29144	Information technology – Biometrics – The use of biometric technology in commercial Identity Management applications and processes
ISO/IEC/TR 29196	Guidance for biometric enrolment
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap Part 2: Architectural components and maturity model
ISO/TR 17424	Intelligent transport systems – Cooperative systems – State of the art of Local Dynamic Maps concepts – CORR: June 30, 2015
ISO/TR 17427-3	Intelligent transport systems – Cooperative ITS Part 3: Concept of operations (ConOps) for 'core' systems
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/TR 17427-9	Intelligent transport systems – Cooperative ITS Part 9: Compliance and enforcement aspects
ISO/TR 17465-2	Intelligent transport systems – Cooperative ITS – Part 2: Guidelines for standards documents
ISO/TR 18638	Health informatics – Guidance on health information privacy education in healthcare organizations
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – CORR: February 28, 2014
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
ISO/TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care (ISO/TS 19256:2016); English version CEN ISO/TS 19256:2017
ISO/TS 21089	Health informatics – Trusted end-to-end information flows
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles

ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO/TS 37107	Sustainable cities and communities – Maturity model for smart sustainable communities
ITU-T M.3363	Requirements for data management in the telecommunication management network – Study Group 2
ITU-T SERIES X SUPP 32	ITU-T X.1058 – Supplement on code of practice for personally identifiable information (PII) protection for telecommunications organizations – Study Group 17
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T SERIES Y SUPP 56	ITU-T Y-series – Supplement on use cases of smart cities and communities – Study Group 20
ITU-T X.1045	Security service chain architecture for networks and applications – Study Group 17
ITU-T X.1209	Capabilities and their context scenarios for cybersecurity information sharing and exchange – Study Group 17
ITU-T X.1361	Security framework for the Internet of things based on the gateway model – Study Group 17
ITU-T X.1363	(Pre-Published) Technical framework of personally identifiable information (PII) handling in Internet of things (IoT) environment
ITU-T Y.2705	Minimum security requirements for the interconnection of the Emergency Telecommunications Service (ETS) – Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3519	Cloud computing – Functional architecture of big data as a service – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.4117	Requirements and capabilities of the Internet of things for support of wearable devices and related services – Study Group 20
ITU-T Y.4500.2	oneM2M – Requirements – Study Group 20
ITU-T Y.4555	Service functionalities of self-quantification over Internet of things – Study Group 20
ITU-T Y.4904	Smart sustainable cities maturity model – Study Group 20
SAE AIR6904	Rationale, Considerations, and Framework for Data Interoperability for Health Management within the Aerospace Ecosystem
SAE EIA-836B	Configuration Management Data Exchange and Interoperability – Formerly TechAmerica EIA-836B; Includes Access to Additional Content
SNZ HB 246	Guidelines for managing risk in sport and recreation organizations
UL 2800 BULLETIN	UL Standard for Safety Medical Device Interoperability – COMMENTS DUE: November 5, 2018
ULC CAN/ULC-S576	STANDARD FOR MASS NOTIFICATION SYSTEM EQUIPMENT AND ACCESSORIES – SECOND EDITION
ISO TR 14872	Health informatics – Identification of medicinal products – Core principles for maintenance of identifiers and terms – First edition
ISO 18750	Intelligent transport systems – Co-operative ITS – Local dynamic map – First Edition
ISO/IEC TR 20748-1	Information technology for learning, education and training – Learning analytics interoperability – Part 1: Reference model – First Edition
ETSI TS 102 573	Electronic Signatures and Infrastructures (ESI); Policy requirements for trust service providers signing and/or storing data objects – V2.1.1
AWWA G430	Security Practices for Operation and Management
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada

CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
IEEE P3333.2.3	Standard for Three-Dimensional (3D) Medical Data Management

Issue 26 — Encryption

ANSI INCITS 504-1	Information Technology – Generic Identity Command Set – Part 1: Card Application Command Set
ANSI INCITS 504-3	Information Technology – Generic Identity Command – Part 3: GICS Platform Testing Requirements
ANSI X9 TR-48	Card-Not-Present (CNP) Fraud Mitigation in the United States: Strategies for Preventing, Detecting, and Responding to a Growing Threat – ASCX9
ANSI X9.69	Framework for Key Management Extensions
ANSI X9.73	Cryptographic Message Syntax – ASN.1 and XML – ASCX9
ASHRAE 135	BACnet – A Data Communication Protocol for Building Automation and Control Networks
ASHRAE HVAC APPLICATIONS SI CH 40	COMPUTER APPLICATIONS
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code of practice for implementation of BS 10008-1
BSI DD ENV 13608-1	Health Informatics – Security for Healthcare Communication – Part 1: Concepts and Terminology
BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
BSI PD CEN/TR 16742	Intelligent transport systems – Privacy aspects in ITS standards and systems in Europe
CEN 15320	Identification card systems – Surface transport applications – Interoperable Public Transport Applications – Framework
CEN 15531-2	Public transport – Service interface for real-time information relating to public transport operations – Part 2: Communications; English version EN 15531-2:2015
CEN 16312	Intelligent transport systems – Automatic Vehicle and Equipment Registration (AVI/AEI) – Interoperable application profile for AVI/AEI and Electronic Register Identification using dedicated short range communication; English version EN 16312:2013
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
CSA PLUS 8830-95	Implementing Privacy Codes of Practice
DIN 66398	Guideline for development of a concept for data deletion with derivation of deletion periods for personal identifiable information
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN CEN/TS 16634	Personal identification – Recommendations for using biometrics in European Automated Border Control; English version CEN/TS 16634:2014
ETSI GR NFV 001	Network Functions Virtualisation (NFV); Use Cases – V1.2.1
ETSI GR NFV-SEC 003	Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance – V1.2.1
ETSI GR NFV-SEC 009	Network Functions Virtualisation (NFV); NFV Security; Report on use cases and technical approaches for multi-layer host administration – V1.2.1

ETSI GR QSC 001	Quantum-Safe Cryptography (QSC); Quantum-safe algorithmic framework – V1.1.1
ETSI GR QSC 003	Quantum Safe Cryptography; Case Studies and Deployment Scenarios – V1.1.1
ETSI GR QSC 004	Quantum-Safe Cryptography; Quantum-Safe threat assessment – V1.1.1
ETSI GR QSC 006	Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes – V1.1.1
ETSI GS ENI 005	Experiential Networked Intelligence (ENI); System Architecture – V1.1.1
ETSI GS INS 005	Identity and access management for Networks and Services; Requirements of an Enforcement Framework in a Distributed Environment – V1.1.1
ETSI GS NFV-SEC 001	Network Functions Virtualisation (NFV); NFV Security; Problem Statement – V1.1.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns – V1.1.1
ETSI GS NFV-SEC 013	Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification – V3.1.1
ETSI GS NGP 001	Next Generation Protocols (NGP); Scenario Definitions – V1.3.1
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI TR 102 935	Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform – V2.1.1
ETSI TR 103 304	CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services – V1.1.1
ETSI TR 103 305	CYBER; Critical Security Controls for Effective Cyber Defence – V1.1.1
ETSI TR 103 305-1	CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls – V3.1.1
ETSI TR 103 305-3	CYBER; Critical Security Controls for Effective Cyber Defence; Part 3: Service Sector Implementations – V2.1.1
ETSI TR 103 308	CYBER; Security baseline regarding LI and RD for NFV and related platforms – V1.1.1
ETSI TR 103 376	SmartM2M; IoT LSP use cases and standards gaps – V1.1.1
ETSI TR 103 456	CYBER; Implementation of the Network and Information Security (NIS) Directive – V1.1.1
ETSI TR 103 509	SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well – V1.1.1
ETSI TR 103 533	SmartM2M; Security; Standards Landscape and best practices – V1.1.1
ETSI TR 103 591	SmartM2M; Privacy study report; Standards Landscape and best practices – V1.1.1
ETSI TS 102 412	Smart Cards; Smart Card Platform Requirements Stage 1 – V12.1.0; Release 12
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI GS MOI 002	Measurement Ontology for IP traffic (MOI); Requirements for IP traffic measurement ontologies development – V1.1.1
ETSI TR 102 935	Machine-to-Machine communications (M2M); Applicability of M2M architecture to Smart Grid Networks; Impact of Smart Grids on M2M platform – V2.1.1
ETSI TS 118 103	oneM2M; Security solutions – V2.4.1; oneM2M TS-0003 version 2.4.1 Release 2
ETSI TR 103 582	EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations – V1.1.1
ETSI TS 103 485	CYBER; Mechanisms for privacy assurance and verification – V1.1.1
ETSI TR 102 937	eCall communications equipment; Conformance to EU vehicle regulations, R&TTE, EMC & LV Directives, and EU regulations for eCall implementation – V1.1.1

IEC 62443-2-4	Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers
IEC 62443-3-3	Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels
IEC 62443-4-2	Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components
IEC/TR 62939-1	Smart grid user interface – Part 1: Interface overview and country perspectives – Edition 1.0
IEC/TS 62045-1	Multimedia security – Guideline for privacy protection of equipment and systems in and out of use – Part 1: General
IEEE 1619	Cryptographic Protection of Data on Block- Oriented Storage Devices – IEEE Computer Society
IEEE 1619.2	Wide-Block Encryption for Shared Storage Media – IEEE Computer Society
IEEE 1703	Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables
IEEE 23026	Systems and software engineering – Engineering and management of websites for systems, software, and services information
IEEE 2410	Biometric Open Protocol
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	PHD Cybersecurity Standards Roadmap – Version: 1.0
IEEE 2600	Information Technology: Hardcopy Device and System Security – IEEE Computer Society
ISO 11073-90101	Health informatics – Point-of-care medical device communication – Part 90101: Analytical instruments – Point-of-care test
ISO 16484-3	Building automation and control systems (BACS) – Part 3: Functions
ISO 16484-5	Building automation and control systems (BACS) Part 5: Data communication protocol – AMD: May 31, 2020
ISO 20214	Space data and information transfer systems – Security architecture for space data systems
ISO TR 11636	Health Informatics – Dynamic on-demand virtual private network for health information infrastructure – First Edition
ISO TR 17427-3	Intelligent transport systems – Cooperative ITS – Part 3: Concept of operations (ConOps) for 'core' systems – First Edition
ISO TR 23244	Blockchain and distributed ledger technologies – Privacy and personally identifiable information protection considerations – First edition
ISO TR 23455	Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems – First edition
ISO TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – First Edition
ISO TS 21089	Health informatics – Trusted end-toend information flows – First Edition
ISO TS 22220	Health informatics – Identification of subjects of health care – Second Edition
ISO TS 29585	Health informatics – Deployment of a clinical data warehouse – First Edition
ISO/IEC 15408-2	Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional components (ISO/IEC 15408-2:2008)
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture
ISO/IEC 18033-6	IT Security techniques – Encryption algorithms – Part 6: Homomorphic encryption
ISO/IEC 20889	Privacy enhancing data de-identification terminology and classification of techniques
ISO/IEC 25023	Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – Measurement of system and software product quality

ISO/IEC 27017	Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services
ISO/IEC 27033-1	Information technology – Security techniques – Network security – Part 1: Overview and concepts
ISO/IEC 27033-3	Information technology – Security techniques – Network security Part 3: Reference networking scenarios – Threats, design techniques and control issues
ISO/IEC 27040	Information technology – Security techniques – Storage security – CORR: September 30, 2016
ISO/IEC 27050-1	Information technology – Electronic discovery Part 1: Overview and concepts
ISO/IEC 29101	Information technology – Security techniques – Privacy architecture framework
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiable information protection – First Edition
ISO/IEC 30118-2	Information technology – Open Connectivity Foundation (OCF) Specification Part 2: Security specification
ISO/IEC 30136	Information technology – Performance testing of biometric template protection schemes
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TR 22678	Information technology – Cloud computing – Guidance for policy development
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence – First edition
ISO/IEC TR 24714-1	Information technology – Biometrics – Jurisdictional and societal considerations for commerical applications Part 1: General guidance
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 29181-2	Information technology – Future Network – Problem statement and requirements Part 2: Naming and addressing
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing
ISO/IEC TR 30166	Internet of Things (IoT) – Industrial IoT
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TS 20540	Information technology – Security techniques – Testing cryptographic modules in their operational environment
ISO/IEC TS 23167	Information technology – Cloud computing – Common technologies and techniques
ISO/IEC/IEEE 23026	Systems and software engineering – Engineering and management of websites for systems, software, and services information
ISO/TR 11636	Health Informatics – Dynamic on-demand virtual private network for health information infrastructure
ISO/TR 17427-3	Intelligent transport systems – Cooperative ITS Part 3: Concept of operations (ConOps) for 'core' systems
ISO/TR 18307	Health informatics interoperability and compatibility in messaging and communication standards Key characteristics
ISO/TR 21548	Health informatics – Security requirements for archiving of electronic health records – Guidelines
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment
ISO/TS 21089	Health informatics – Trusted end-to-end information flows
ISO/TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles
ISO/TS 22220	Health informatics – Identification of subjects of health care
ISO/TS 27790	Health informatics – Document registry framework

ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO 25237	Health informatics – Pseudonymization
ISO/IEC TS 27008 – TC	TC – Tracked Changes (Redline) – Information technology – Security techniques – Guidelines for the assessment of information security controls – Compares PD ISO/IEC TS 27008:2019 with PD ISO/IEC TR 27008:2011
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – First Edition
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ISO/TS 14265	Health Informatics – Classification of purposes for processing personal health information
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse
ISO/TS 17975	Health informatics – Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
ISO 22857	Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health data – Second Edition
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/IEC TS 20748-4:20	Information technology for learning, education and training – Learning analytics interoperability – Part 4: Privacy and data protection policies
ISO/IEC 27011	Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations
ISO/IEC 29100	Information technology – Security techniques – Privacy framework (ISO/IEC 29100:2011, including Amd 1:2018)
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment
ISO 5127	Information and documentation Vocabulary
ISO 27799	Health informatics – Information security management in health using ISO/IEC 27002
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/IEC 19506	Information technology – Object Management Group Architecture-Driven Modernization (ADM) – Knowledge Discovery Meta-Model (KDM)
ISO/IEC 27034-1	Information technology – Security techniques – Application security Part 1: Overview and concepts – CORR: February 28, 2014
ISO/IEC 29151	Information technology – Security techniques – Code of practice for personally identifiable information protection
ITU-T H.810	(Pre-Published) Interoperability design guidelines for personal connected health systems: Introduction
ITU-T J.191	IP feature package to enhance cable modems
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T X.1039	Technical security measures for implementation of ITU-T X.805 security dimensions – Study Group 17
ITU-T X.1045	Security service chain architecture for networks and applications – Study Group 17
ITU-T X.1361	Security framework for the Internet of things based on the gateway model – Study Group 17
ITU-T X.1401	Security threats to distributed ledger technology – Study Group 17
ITU-T X.1602	Security requirements for software as a service application environments – Study Group 17
ITU-T X.1642	Guidelines for the operational security of cloud computing – Study Group 17
ITU-T X.894	(Pre-Published) Generic applications of ASN.1 Cryptographic Message Syntax
ITU-T Y.2342	Scenarios and capability requirements of blockchain in next generation network evolution – Study Group 13

ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ITU-T Y.3505	Cloud computing – Overview and functional requirements for data storage federation – Study Group 13
ITU-T Y.3509	Cloud computing – Functional architecture for data storage federation – Study Group 13
ITU-T Y.3518	Cloud computing – Functional requirements of inter-cloud data management – Study Group 13
ITU-T Y.3524	Cloud computing maturity requirements and framework – Study Group 13
ITU-T Y.3800	Overview on networks supporting quantum key distribution Corrigendum 1 – Study Group 13
ITU-T Y.4459	Digital entity architecture framework for Internet of things interoperability – Study Group 20
ITU-T Y.3501	Cloud computing – Framework and high-level requirements – Study Group 13
ITU-T H.780	Digital signage: Service requirements and IPTV-based architecture – Study Group 16
NEMA C12.22	Protocol Specification for Interfacing to Data Communication Networks
UL CAN/UL 2900-1	UL Standard for Safety Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements – First Edition; Reprint with Revisions Through and Including June 5, 2020
UL SUBJECT 2900-1	UL Outline for Investigation Software Cybersecurity for Network- Connectable Products, Part 1: General Requirements – Issue 2

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 103-1:2020	Digital trust and identity – Part 1: Fundamentals
CAN/CIOSC 103-2	Digital identity and trust – Part 2: Delivery of health care services
IEEE Std 2410-2019	IEEE Standard for Biometric Open Protocol
IEEE Std 1363.3-2013	IEEE Standard for Identity-Based Cryptographic Techniques using Pairings
IEEE 1619.1-2018	IEEE Standard for Authenticated Encryption with Length Expansion for Storage Devices
IEEE 1735-2014	IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP)
IEEE P802.15.4y	IEEE Draft Standard for Low-Rate Wireless Networks Amendment Defining Support for Advanced Encryption Standard (AES)-256 Encryption and Security Extensions
IEEE 802.1AEcg-2017	IEEE Standard for Local and metropolitan area networks – Media Access Control (MAC) Security – Amendment 3: Ethernet Data Encryption devices
IEEE/ISO/IEC 8802-1AE:2013/Amd.3-2018 -	IEEE/ISO/IEC International Standard – Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Part 1AE: Media access control (MAC) security AMENDMENT 3: Ethernet data encryption devices
IEEE 1609.2b-2019	IEEE Standard for Wireless Access in Vehicular Environments – Security Services for Applications and Management Messages – Amendment 2 – PDU Functional Types and Encryption Key Management
IEEE 8802-1AE:2013/Amd.1-2015	ISO/IEC/IEEE International Standard for Information technology – Telecommunications and information exchan+F43ge between systems – Local and metropolitan area networks – Part 1AE: Media access control (MAC) security – AMENDMENT 1: Galois Counter Model – Advanced Encryption Standard-256 (GCMAES-256) Cipher Suite
IEEE ST 429-6:2006 Am1:2018	SMPTE Amendment – D-Cinema Packaging – MXF Track File Essence Encryption

Issue 27 —
Management of ontologies

ITU-T Y.2076	Semantics based requirements and framework of the Internet of things – Study Group 13
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ITU-T Y.4203	Requirements of things description in the Internet of things – Study Group 20
ITU-T Y.4461	Framework of open data in smart cities – Study Group 20
ISO/TS 13606-4	Health informatics – Electronic health record communication – Part 4: Security
ETSI TR 103 537	SmartM2M; Plugtests™ preparation on Semantic Interoperability – V1.1.1
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
ETSI GS MOI 010	Measurement Ontology for IP traffic (MOI); Report on information models for IP traffic measurement – V1.1.1
ANSI INCITS 532	Information Technology – Vocabulary Description and Management
DIN SPEC 91349	Taxonomy of Rules and Regulations in Smart Data; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach – V1.1.1
ETSI TR 103 411	SmartM2M; Smart Appliances; SAREF extension investigation – V1.1.1
ETSI TR 103 509	SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well – V1.1.1
ISO 13606-1	Health informatics – Electronic health record communication – Part 1: Reference model (ISO 13606-1:2019); English version EN ISO 13606-1:2019
ISO 8000-115	Data quality – Part 115: Master data: Exchange of quality identifiers: Syntactic, semantic and resolution requirements – First Edition
ISO 8000-116	Data quality Part 116: Master data: Exchange of quality identifiers: Application of ISO 8000-115 to authoritative legal entity identifiers
ISO 8000-120	Data quality – Part 120: Master data: Exchange of characteristic data: Provenance – First Edition
ISO 8000-130	Data quality – Part 130: Master data: Exchange of characteristic data: Accuracy – First Edition
ISO 8000-140	Data quality – Part 140: Master data: Exchange of characteristic data: Completeness – First Edition
ISO 8000-2	Data quality Part 2: Vocabulary
ISO/IEC 11179-1	Information technology – Specification and standardization of data elements – Part 1: Framework for the specification and standardization of data elements
ISO/IEC 11179-3	Information technology – Metadata registries (MDR) – Part 3: Registry metamodel and basic attributes
ISO/IEC 11179-5	Information technology – Metadata registries (MDR) – Part 5: Naming and Identification principles
ISO/IEC 11179-6	Information technology – Metadata registries (MDR) Part 6: Registration
ISO/IEC 11179-7	Information technology – Metadata registries (MDR) – Part 7: Metamodel for data set registration
ISO/IEC 15026.1	Systems and software engineering – Systems and software assurance Part 1: Concepts and vocabulary
ISO/IEC 16680	Information technology – The Open Group Service Integration Maturity Model (OSIMM)
ISO/IEC 19763-1	Information technology – Metamodel framework for interoperability (MFI) – Part 1: Reference model
ISO/IEC 19763-3	Information technology – Metamodel framework for interoperability (MFI) – Part 3: Metamodel for ontology registration
ISO/IEC 19763-5	Information technology – Metamodel framework for interoperability (MFI) – Part 5: Metamodel for process model registration
ISO/IEC 19763-6	Information technology – Metamodel framework for interoperability (MFI) – Part 6: Registry Summary – First Edition

ISO/IEC 19763-7	Information technology – Metamodel framework for interoperability (MFI) – Part 7: Metamodel for service model registration
ISO/IEC 20547-3	Information technology – Big data reference architecture Part 3: Reference architecture
ISO/IEC 24707	Information technology – Common Logic (CL): a framework for a family of logic-based languages
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability
ISO/IEC TR 19583-1	Information technology – Concepts and usage of metadata Part 1: Metadata concepts
ISO/IEC TR 20547-5	Information technology – Big data reference architecture – Part 5: Standards roadmap
ISO/IEC TR 20943-1	Information technology Procedures for achieving metadata registry (MDR) content consistency Part 1: Data elements
ISO/IEC TR 20943-5	Information technology – Procedures for achieving metadata registry content consistency – Part 5: Metadata mapping procedure – First Edition
ISO/IEC TR 20943-6	Information technology – Procedures for achieving metadata registry content consistency – Part 6: Framework for generating ontologies – First Edition
ISO/IEC TS 19763-13	Information technology – Metamodel framework for interoperability (MFI) Part 13: Metamodel for form design registration
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
IEEE Std 2755-2017	IEEE Guide for Terms and Concepts in Intelligent Process Automation
IEEE Std 1636.1-2018	IEEE Standard for Software Interface for Maintenance Information Collection and Analysis (SIMICA): Exchanging Test Results and Session Information via the eXtensible Markup Language (XML)
IEEE 11073-10101-2019	ISO/IEEE International Standard – Health informatics – Point-of-care medical device communication – Part 10101: Nomenclature AMENDMENT 1: Additional definitions
ISO/IEC/IEEE 24765:2017	Systems and software engineering – Vocabulary

Issue 28 —
Data transparency, lineage, and traceability

ANSI INCITS 442	Information Technology – Biometric Identity Assurance Services (BIAS)
ASTM C1009 REV A	Standard Guide for Establishing and Maintaining a Quality Assurance Program for Analytical Laboratories Within the Nuclear Industry
ASTM E1714	Standard Guide for Properties of a Universal Healthcare Identifier (UHID)
ASTM E1931	Standard Guide for Non-computed X-Ray Compton Scatter Tomography
BSI BS 8593	Code of practice for the deployment and use of Body Worn Video (BWV)
BSI PAS 180	Smart cities – Vocabulary
BSI PAS 212	Automatic resource discovery for the Internet of Things – Specification – CORR: November 2016
CGSB CAN/CGSB-72.34	Electronic records as documentary evidence
CSA PLUS 8300-96	Making the CSA Privacy Code Work for You – Includes Plus 8830-95
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
ETSI GR PDL 001	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies – V1.1.1
ETSI GS CIM 006	Context Information Management (CIM); Information Model (MODO) – V1.1.1

ETSI GS CIM 009	Context Information Management (CIM); NGSI-LD API – V1.2.2
ETSI GS INS 005	Identity and access management for Networks and Services; Requirements of an Enforcement Framework in a Distributed Environment – V1.1.1
ETSI GS INS 008	Identity and access management for Networks and Services (INS); Distributed access control enforcement framework; Architecture – V1.1.1
ETSI TR 103 535	SmartM2M; Guidelines for using semantic interoperability in the industry – V1.1.1
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms – V1.1.2
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TS 101 533-1	Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management – V1.3.1
ISO 16175-2	Information and documentation – Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for digital records management systems
ISO 21965	Information and documentation – Records management in enterprise architecture
ISO 25237	Health informatics – Pseudonymization – First Edition
ISO 30401	Knowledge management systems – Requirements.
ISO 5841-2	Implants for Surgery – Cardiac Pacemakers – Part 2: Reporting of Clinical Performance of Populations of Pulse Generators or Leads
ISO TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap – Part 2: Architectural components and maturity model – First Edition
ISO TR 19669	Health informatics – Re-usable component strategy for use case development – First Edition
ISO TR 21965	Information and documentation – Records management in enterprise architecture – First edition
ISO TR 22221	Health informatics Good principles and practices for a clinical data warehouse – First Edition
ISO TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care – First Edition
ISO/IEC 19763-1	Information technology – Metamodel framework for interoperability (MFI) Part 1: Framework
ISO/IEC 30108-1	Information technology – Biometric Identity Assurance Services – Part 1: BIAS services – First Edition; Corrected version 04-15-2016
ISO/IEC 30182	Smart city concept model – Guidance for establishing a model for data interoperability
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC 38505-1	Information technology – Governance of IT – Governance of data – Part 1: Application of ISO/IEC 38500 to the governance of data – First Edition
ISO/IEC TR 16501	Information technology – Generic digital audio-visual systems
ISO/IEC TR 20547-2	Information technology – Big data reference architecture Part 2: Use cases and derived requirements
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence – First edition
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/TR 14639-2	Health informatics – Capacity-based eHealth architecture roadmap – Part 2: Architectural components and maturity model
ISO/TR 19669	Health informatics – Re-usable component strategy for use case development
ISO/TR 22221	Health informatics Good principles and practices for a clinical data warehouse

ISO/TS 19256	Health informatics – Requirements for medicinal product dictionary systems for health care
ISO/TS 29585	Health informatics – Deployment of a clinical data warehouse
ITU-T X.1602	Security requirements for software as a service application environments – Study Group 17
ITU-T Y.3505	Cloud computing – Overview and functional requirements for data storage federation – Study Group 13
ITU-T Y.3509	Cloud computing – Functional architecture for data storage federation – Study Group 13
ITU-T Y.3602	Big data – Functional requirements for data provenance – Study Group 13
ITU-T Y.4464	(Pre-Published) Framework of blockchain of things as decentralized service platform
SAE PT-186/11	Collision Reconstruction Methodologies Volume 11: Biomechanics – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SNZ AS/NZS 5667.1	Water Quality – Sampling Part 1: Guidance on the Design of Sampling Programs, Sampling Techniques and the Preservation and Handling of Samples
SNZ NZS 5259	Gas measurement
SNZ SA/SNZ HB 168	Document control
UL 2800 BULLETIN	UL Standard for Safety Medical Device Interoperability – COMMENTS DUE: November 5, 2018
BSI BS 7958 – TC	TC – Tracked Changes (Redline) – Closed circuit television (CCTV) – Management and operation – Code of practice – Compares BS 7958:2015 with BS 7958:2009
CEN EN 9300-002	Aerospace series – LOTAR -LOng Term Archiving and Retrieval of digital technical product documentation such as 3D, CAD and PDM data – Part 002: Requirements
ISO 13606-1 – TC	TC – Tracked Changes (Redline) – Health informatics – Electronic health record communication Part 1: Reference model – Compares BS EN ISO 13606-1:2019 with BS EN ISO 13606-1:2012
ISO 21090	Health Informatics – Harmonized data types for information interchange
ISO 13606-1	Health informatics – Electronic health record communication – Part 1: Reference model (ISO 13606-1:2019)
ISO/IEC TR 19583-23	Information technology – Concepts and usage of metadata – Part 23: Data element exchange (DEX) for a subset of ISO/IEC 11179-3 – First Edition
IEEE 2804	Standard for Software-Hardware Interface for Multi-Many-Core – IEEE Computer Society
ITU-T Y.3600	Big data – Cloud computing based requirements and capabilities – Study Group 13
ISO/IEC 17913	Information technology – 12,7mm 128-track magnetic tape cartridge for information interchange – Parallel serpentine format
ASTM MNL19	Manual on the Building of Materials Databases
IEEE 1636	Software Interface for Maintenance Information Collection and Analysis (SIMICA)
IEEE 1636.1	Software Interface for Maintenance Information Collection and Analysis (SIMICA): Exchanging Test Results and Session Information via the eXtensible Markup Language (XML)
IEEE 1636.2	Standard for Software Interface for Maintenance Information Collection and Analysis (SIMICA): Exchanging Maintenance Action Information via the Extensible Markup Language (XML)
ISO 22600-1	Health informatics – Privilege management and access control – Part 1: Overview and policy management
ANSI INCITS 315	Information Technology – Magnetic Tape and Cartridge for Information Interchange – Unrecorded, 128-Track, Parallel Serpentine, 12.65 mm (1/2 in), 2550 ftpmm (64 770 ftpi)
ISO 10303-232	Industrial Automation Systems and Integration – Product Data Representation and Exchange – Part 232: Application Protocol: Tehcnical Data Packaging Core Information and Exchange – First Edition
CEN/TR 16742	Intelligent transport systems – Privacy aspects in ITS standards and systems in Europe
CSA Z8002-14	Operation and maintenance of health care facilities – Second edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
IEEE Std 1857.6-2018	IEEE Standard for Digital Media Content Description
CSA Z8003	Health care design research and evaluation

Issue 29 —
Data portability and mobility

BSI BS 10012 + A1	Data protection – Specification for a personal information management system – AMD: July 2018
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI PAS 1040	Digital readiness – Adopting digital technologies in manufacturing – Guide
BSI PAS 1085	Manufacturing – Establishing and implementing a security-minded approach – Specification
BSI PAS 1296	Online age checking – Provision and use of online age check services – Code of practice
BSI PAS 183	Smart cities – Guide to establishing a decision-making framework for sharing data and information services
BSI PAS 185	Smart cities – Specification for establishing and implementing a security-minded approach – CORR: May 30, 2018
BSI PAS 1885	The fundamental principles of automotive cyber security – Specification
BSI PAS 201	Supporting fintechs in engaging with financial institutions – Guide
BSI PAS 92	Code of practice for the implementation of a biometric system
BSI PD CEN/TR 16931-4	Electronic invoicing Part 4: Guidelines on interoperability of electronic invoices at the transmission level
BSI PD CEN/TR 17143	Intelligent transport systems – Standards and actions necessary to enable urban infrastructure coordination to support Urban-ITS
BSI PD CEN/TR 17475	Space – Use of GNSS-based positioning for road Intelligent Transport System (ITS) – Specification of the test facilitities, definition of test scenarios,description and validation of the procedures for field test related to security performance of GNSS-based positioning terminals
BSI PD CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
CEN EN 16234-1	e-Competence Framework (e-CF) – A common European Framework for ICT Professionals in all sectors Part 1: Framework
CEN/TS 17288	Health informatics – The International Patient Summary – Guideline for European Implementation
CSA CSA-Q830-03	Model Code for the Protection of Personal Information – Second Edition
DIN SPEC 4997	Privacy by Blockchain Design: A standardised model for processing personal data using blockchain technology; Text in English
DIN SPEC 91347	Integrated multi-functional Humble Lamppost (imHLa)
DIN SPEC 91357	Reference Architecture Model Open Urban Platform (OUP); Text in English
DIN SPEC 91367	Urban mobility data collection for real-time applications; Text in English

DIN SPEC 91406	Automatic identification of physical objects and information on physical objects in IT systems, particularly IoT systems; Text in German and English
DS DS/CEN/TR 17439	Guidance on how to implement EN ISO 19650-1 and -2 in Europe
DS DS/CEN/TR 17475	Space – Use of GNSS-based positioning for road Intelligent Transport System (ITS) – Specification of the test facilities, definition of test scenarios, description and validation of the procedures for field tests related to security performance of GNSS-based positioning terminals
DS DS/CWA 16871-1	Requirements and Recommendations for Assurance in Cloud Security – Part 1: Contributed recommendations from European projects
EN 319 531	Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Registered Electronic Mail Service Providers – V1.1.1
EN 319 532-1	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 1: Framework and architecture – V1.1.1
EN 319 532-2	Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM) Services; Part 2: Semantic contents – V1.1.1
ETSI GR CIM 002	Context Information Management (CIM); Use Cases (UC) – V1.1.1
ETSI GR ENI 007	Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks – V1.1.1
ETSI GR PDL 001	Permissioned Distributed Ledger (PDL); Landscape of Standards and Technologies – V1.1.1
ETSI GR ZSM 004	Zero-touch network and Service Management (ZSM); Landscape – V1.1.1
ETSI GS NFV-SEC 006	Network Functions Virtualisation (NFV); Security Guide; Report on Security Aspects and Regulatory Concerns – V1.1.1
ETSI SR 003 381	Cloud Standards Coordination Phase 2; Identification of Cloud user needs – V2.1.1
ETSI SR 003 391	Cloud Standards Coordination Phase 2; Interoperability and Security in Cloud Computing – V2.1.1
ETSI SR 003 392	Cloud Standards Coordination Phase 2; Cloud Computing Standards Maturity Assessment; A new snapshot of Cloud Computing Standards – V2.1.1
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach – V1.1.1
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 370	Practical introductory guide to Technical Standards for Privacy – V1.1.1
ETSI TR 103 477	eHEALTH; Standardization use cases for eHealth – V1.1.1
ETSI TR 103 509	SmartM2M; SAREF extension investigation; Requirements for eHealth/Ageing-well – V1.1.1
ETSI TR 103 533	SmartM2M; Security; Standards Landscape and best practices – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms – V1.1.2
ETSI TR 103 582	EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations – V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TR 119 500	Business Driven Guidance for Trust Application Service Providers – V1.1.1
ETSI TS 102 223	Smart Cards; Card Application Toolkit (CAT) – V15.3.0; Release 15
ETSI TS 103 458	CYBER; Application of Attribute Based Encryption (ABE) for PII and personal data protection on IoT devices, WLAN, cloud and mobile services – High level requirements – V1.1.1
ETSI TS 103 532	CYBER; Attribute Based Encryption for Attribute Based Access Control – V1.1.1
ETSI TS 103 643	Techniques for assurance of digital material used in legal proceedings – V1.1.1

ETSI TS 132 421	Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Telecommunication management; Subscriber and equipment trace; Trace concepts and requirements – V15.3.0; 3GPP TS 32.421 version 15.3.0 Release 15
IEC 61800-7-202	Adjustable speed electrical power drive systems – Part 7-202: Generic interface and use of profiles for power drive systems – Profile type 2 specification – Edition 2.0
IEEE 1900 SERIES	Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management – Includes IEEE 1900.1, IEEE 1900.2, IEEE 1900.4, IEEE 1900.4a, IEEE 1900.4.1, IEEE 1900.5, IEEE 1900.5.2, IEEE 1900.6, IEEE 1900.6A, IEEE 1900.7
IEEE 1934	Adoption of OpenFog Reference Architecture for Fog Computing
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being
IEEE NEUROTECHNOLOGIES BMI ROADMAP	STANDARDS ROADMAP: NEUROTECHNOLOGIES FOR BRAIN-MACHINE INTERFACING
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	PHD Cybersecurity Standards Roadmap – Version: 1.0
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 10617	Textiles – Standard data format for colorimetric communication – Textiles and related measurements
ISO 10667-2	Assessment service delivery – Procedures and methods to assess people in work and organizational settings Part 2: Requirements for service providers
ISO 13606-4	Health informatics – Electronic health record communication – Part 4: Security – First edition
ISO 17115	Health informatics – Representation of categorial structures of terminology (CatStructure)
ISO 17117-1	Health informatics – Terminological resources – Part 1: Characteristics
ISO 18308	Health informatics – Requirements for an electronic health record architecture
ISO 18750	Intelligent transport systems – Co-operative ITS – Local dynamic map (ISO 18750:2018)
ISO 19465	Traditional Chinese medicine – Categories of traditional Chinese medicine (TCM) clinical terminological systems
ISO 19626-1	Processes, data elements and documents in commerce, industry and administration – Trusted communication platforms for electronic documents Part 1: Fundamentals
ISO 20264	Stationary source emissions – Determination of the mass concentration of individual volatile organic compounds (VOCs) in waste gases from non-combustion processes – First edition
ISO 22367	Medical laboratories – Application of risk management to medical laboratories – CORR: May 31, 2020
ISO 23354	Business requirements for end-toend visibility of logistics flow
ISO 25237	Health informatics – Pseudonymization – First Edition
ISO 26000	Guidance on social responsibility (ISO 26000:2010)
ISO 37156	Smart community infrastructures – Guidelines on data exchange and sharing for smart community infrastructures
ISO IWA 31	Risk management – Guidelines on using ISO 31000 in management systems
ISO TR 24971	Medical devices – Guidance on the application of ISO 14971 – Second edition (STANDARD PLUS REDLINE)
ISO TS 16843-1	Health informatics – Categorial structures for representation of acupuncture – Part 1: Acupuncture points – First Edition
ISO TS 16843-2	Health informatics – Categorial structures for representation of acupuncture – Part 2: Needling – First Edition

ISO TS 16843-3	Health informatics – Categorial structures for representation of acupuncture – Part 3: Moxibustion – First Edition
ISO TS 16843-4	Health informatics – Categorial structures for representation of acupuncture – Part 4: Meridian and collateral channels – First Edition
ISO TS 16843-5	Health Informatics – Categorial structures for representation of acupuncture – Part 5: Cupping – First Edition
ISO TS 18101-1	Automation systems and integration – Oil and gas interoperability – Part 1: Overview and fundamental principles – First edition
ISO TS 18790-1	Health informatics – Profiling framework and classification for Traditional Medicine informatics standards development – Part 1: Traditional Chinese Medicine – First Edition
ISO TS 19299	Electronic fee collection – Security framework – First Edition
ISO TS 19844	Health informatics – Identification of medicinal products (IDMP) – Implementation guidelines for ISO 11238 for data elements and structures for the unique identification and exchange of regulated information on substances – Third Edition
ISO TS 21192	Electronic fee collection – Support for traffic management – First edition
ISO TS 21547	Health informatics – Security requirements for archiving of electronic health records – Principles – First Edition
ISO TS 21831	Information model of Chinese materia medica processing – First edition
ISO TS 22773	Health Informatics – Categorial structures for the representation of the decocting process in traditional Chinese medicine – First edition
ISO TS 22789	Health informatics – Conceptual framework for patient findings and problems in terminologies – First Edition
ISO TS 22835	Health informatics – Information model of combination of decoction pieces in Chinese medicines – First Edition
ISO TS 22990	Traditional Chinese medicine – Categories of clinical terminological system to support the integration of clinical terms from traditional Chinese medicine and Western medicine – First edition
ISO TS 23303	Health informatics – Categorial structure for Chinese materia medica products manufacturing process – First edition
ISO TS 8000-311	Data quality – Part 311: Guidance for the application of product data quality for shape (PDQ-S) – First Edition
ISO/IEC 12087-5	Information technology Computer graphics and image processing Image Processing and Interchange (IPI) Functional specification Part 5: Basic Image Interchange Format (BIIF)
ISO/IEC 15944-12	Information technology – Business operational view Part 12: Privacy protection requirements (PPR) on information life cycle management (ILCM) and EDI of personal information (PI)
ISO/IEC 17789	Information technology – Cloud computing – Reference architecture (ISO/IEC 17789:2014)
ISO/IEC 18384-2	Information technology – Reference Architecture for Service Oriented Architecture (SOA RA) – Part 2: Reference Architecture for SOA Solutions – First Edition
ISO/IEC 19086-1	Information technology – Cloud computing – Service level agreement (SLA) framework Part 1: Overview and concepts
ISO/IEC 19086-3	Information technology – Cloud computing – Service level agreement (SLA) framework Part 3: Core conformance requirements
ISO/IEC 19286	Identification cards – Integrated circuit cards – Privacy-enhancing protocols and services – First Edition
ISO/IEC 19780-1	Information technology – Learning, education and training – Collaborative technology – Collaborative learning communication – Part 1: Text-based communication
ISO/IEC 19941	Information technology – Cloud computing – Interoperability and portability
ISO/IEC 19944	Information technology – Cloud computing – Cloud services and devices: Data flow, data categories and data use – First Edition

ISO/IEC 20748.2	Information technology for learning, education and training – Learning analytics interoperability Part 2: System requirements
ISO/IEC 21964-1	Information technology – Destruction of data carriers Part 1: Principles and definitions
ISO/IEC 21964-3	Information technology – Destruction of data carriers Part 3: Process of destruction of data carriers
ISO/IEC 22624	Information technology – Cloud computing – Taxonomy based data handling for cloud services – First edition
ISO/IEC 27701	Expert commentary BS ISO/IEC 27701:2019 – Security techniques – Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management – Requirements and guidelines
ISO/IEC 29184	Information technology – Online privacy notices and consent
ISO/IEC 38505.2	Information technology – Governance of IT – Governance of data Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC GUIDE 71	Guide for addressing accessibility in standards
ISO/IEC TR 20547-2	Information technology – Big data reference architecture Part 2: Use cases and derived requirements
ISO/IEC TR 20748-2	Information technology for learning, education and training – Learning analytics interoperability Part 2: System requirements – CORR: August 31, 2018
ISO/IEC TR 22678	Information technology – Cloud computing – Guidance for policy development
ISO/IEC TR 23186	Information technology – Cloud computing – Framework of trust for processing of multi-sourced data
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes
ISO/IEC TR 30164	Internet of things (IoT) – Edge computing
ISO/IEC TR 38505-2	Information technology – Governance of IT – Governance of data – Part 2: Implications of ISO/IEC 38505-1 for data management
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/IEC/IEEE 8802-1AX	Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements Part 1AX: Link Aggregation – First Edition
ISO/TR 17427-7	Intelligent transport systems – Cooperative ITS Part 7: Privacy aspects
ISO/TR 23021	Traditional Chinese medicine – Controlled vocabulary on Japanese Kampo crude drugs
ISO/TR 23022	Traditional Chinese medicine – Controlled vocabulary on Japanese Kampo formulas and the indication codes for the products
ISO/TR 24971	Medical devices – Guidance on the application of ISO 14971
ISO/TS 14441	Health informatics – Security and privacy requirements of EHR systems for use in conformity assessment – CORR: February 28, 2014
ISO/TS 16277-1	Health informatics – Categorial structures of clinical findings in traditional medicine Part 1: Traditional Chinese, Japanese and Korean medicine
ISO/TS 16843-1	Health informatics – Categorial structures for representation of acupuncture – Part 1: Acupuncture points
ISO/TS 16843-3	Health informatics – Categorial structures for representation of acupuncture Part 3: Moxibustion
ISO/TS 16843-4	Health informatics – Categorial structures for representation of acupuncture Part 4: Meridian and collateral channels
ISO/TS 16843-5	Health Informatics – Categorial structures for representation of acupuncture – Part 5: Cupping
ISO/TS 18062	Health informatics – Categorial structure for representation of herbal medicaments in terminological systems
ISO/TS 18101-1	Automation systems and integration – Oil and gas interoperability – Part 1: Overview and fundamental principles
ISO/TS 18750	Intelligent transport systems – Cooperative systems – Definition of a global concept for Local Dynamic Maps (ISO/TS 18750:2015); English version CEN ISO/TS 18750:2015

ISO/TS 18790-1	Health informatics – Profiling framework and classification for Traditional Medicine informatics standards development Part 1: Traditional Chinese Medicine
ISO/TS 21192	Electronic fee collection – Support for traffic management
ISO/TS 21564	Health Informatics – Terminology resource map quality measures (MapQual)
ISO/TS 21831	Information model of Chinese materia medica processing
ISO/TS 22773	Health Informatics – Categorial structures for the representation of the decocting process in traditional Chinese medicine
ISO/TS 22835	Health informatics – Information model of combination of decoction pieces in Chinese medicines
ISO/TS 23303	Health informatics – Categorial structure for Chinese materia medica products manufacturing process
ITU-R M.1457-14	Detailed specifications of the terrestrial radio interfaces of International Mobile Telecommunications-2000 (IMT-2000)
ITU-T G.1032	(Pre-Published) Influence Factors on Gaming Quality of Experience
ITU-T K.81	High-power electromagnetic immunity guide for telecommunication systems – Study Group 5
ITU-T L.1305	Data centre infrastructure management system based on big data and artificial intelligence technology – Study Group 5
ITU-T L.1470	Greenhouse gas emissions trajectories for the information and communication technology sector compatible with the UNFCCC Paris Agreement – Study Group 5
ITU-T SERIES H SUPP 17	Guide for addressing accessibility in standards – Study Group 16
ITU-T SERIES Q SUPP 65	Cloud computing interoperability activities – Study Group 11
ITU-T SERIES Q SUPP 66	Supplement on scenarios and requirements in terms of services and deployments for IMT and IMS in developing countries – Study Group 13
ITU-T SERIES Y SUPP 49	ITU-T Y.3500-series – Cloud computing standardization roadmap – Study Group 15
ITU-T SERIES Y SUPP 52	Methodology for building digital capabilities during enterprises' digital transformation – Study Group 20
ITU-T SERIES Y SUPP 56	ITU-T Y-series – Supplement on use cases of smart cities and communities – Study Group 20
ITU-T Y.3052	Overview of trust provisioning in information and communication technology infrastructures and services – Study Group 13
ITU-T Y.3173	Framework for evaluating intelligence levels of future networks including IMT-2020 – Study Group 13
ITU-T Y.3502	Information technology – Cloud computing – Reference architecture – Study Group 13
ITU-T Y.4003	Overview of smart manufacturing in the context of the industrial Internet of things – Study Group 20
ITU-T Y.4905	(Pre-Published) Smart sustainable city impact assessment
ITU-T Y.4906	Assessment framework for digital transformation of sectors in smart cities – Study Group 20
SAE AIR6904	Rationale, Considerations, and Framework for Data Interoperability for Health Management within the Aerospace Ecosystem
SAE AS5506C	(R) Architecture Analysis & Design Language (AADL)
SAE R-463	Introduction to Advanced Manufacturing – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS	
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-2:2020	Data governance – Part 2: Third party access to data
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CSA Z8003	Health care design research and evaluation

Working Group 4:
Data Analytics, Solutions, and Commercialization

Issue 30 —
Technical Elements of AI Solutions

ANSI INCITS 172	Information Technology – American National Standard Dictionary of Information Technology (ANSDIT)
ANSI X9.112-3	Wireless Management and Security Part 3: Mobile
API PUBL 4452	1987 Oil Spill Conference
ASCE 70-19	Estimation of Aquifer Hydraulic Properties by Inverse Numerical Modeling of Aquifer Pumping Tests
ASCE GSP 199	GEOFLORIDA 2010 ADVANCES IN ANALYSIS, MODELING & DESIGN
ASCE GSP 318	Geo-Congress 2020: Geotechnical Earthquake Engineering and Special Topics
ASHRAE 4692	Development and Implementation of HVAC-KBCD: A Knowledge-Based Expert System for Conceptual Design of HVAC&R System – Part 2: Application to Office Buildings
ASHRAE AB-10-022	To Assess the Validity of the Transfer Function Method: A Neural Model for the Optimal Choice of Conduction Transfer Functions
ASHRAE DATACOM SERIES BOOK 14	Advancing DCIM with IT Equipment Integration
ASHRAE TRAN 2010-2	2010 ASHRAE TRANSACTIONS VOLUME 116 PART 2
ASHRAE TRAN 2019-2	2019 ASHRAE TRANSACTIONS – VOLUME 125, PART 2
ASHRAE TRAN 2020-1	2020 ASHRAE TRANSACTIONS – VOLUME 126 – PART 1
ASTM F2446	Standard Classification for Hierarchy of Equipment Identifiers and Boundaries for Reliability, Availability, and Maintainability (RAM) Performance Data Exchange
ASTM F3060	Standard Terminology for Aircraft
BSI BS 10008-2	Evidential weight and legal admissibility of electronically stored information (ESI) Part 2: Code of practice for implementation of BS 10008-1
BSI BS 10102-1	Big data Part 1: Guidance on data-driven organizations
BSI BS 5192-1	Guide to Production Control – Part 1: Introduction
BSI PAS 1000	Business agility – Concept and framework – Guide
BSI PAS 1040	Digital readiness – Adopting digital technologies in manufacturing – Guide
BSI PAS 1085	Manufacturing – Establishing and implementing a security-minded approach – Specification
BSI PAS 1880	Guidelines for developing and assessing control systems for automated vehicles – FREE DOWLOAND FROM BSI SHOP
BSI PAS 1885	The fundamental principles of automotive cyber security – Specification
BSI PAS 440	Responsible innovation – Guide
BSI PAS 7040	Digital manufacturing – Trustworthiness and precision of networked sensors – Guide
BSI PAS 7340	Framework for embedding the principles of sustainable finance in financial services organizations – Guide
CIE X046 VOL 1-2	PROCEEDINGS of the 29th Session of the CIE Washington D.C., USA, June 14 – 22, 2019 Volume 1 – Part 2
DS DS/CWA 17492	Predictive control and maintenance of data intensive industrial processes
DIN SPEC 92001-1	Artificial Intelligence – Life Cycle Processes and Quality Requirements – Part 1: Quality Meta Model; Text in English

ETSI EG 202 301	Universal Communications Identifier (UCI); Using UCI to enhance communications for disabled, young and elderly people – V1.1.1
ETSI EN 303 470	Environmental Engineering (EE); Energy Efficiency measurement methodology and metrics for servers – V1.1.1
ETSI ES 202 336-12	Environmental Engineering (EE); Monitoring and control interface for infrastructure equipment (power, cooling and building environment systems used in telecommunication networks); Part 12: ICT equipment power, energy and environmental parameters monitoring information model – V1.2.1
ETSI GR ARF 002	Augmented Reality Framework (ARF) Industrial use cases for AR applications and services – V1.1.1
ETSI GR CIM 002	Context Information Management (CIM); Use Cases (UC) – V1.1.1
ETSI GR ENI 003	Experiential Networked Intelligence (ENI); Context-Aware Policy Management Gap Analysis – V1.1.1
ETSI GR ENI 004	Experiential Networked Intelligence (ENI); Terminology for Main Concepts in ENI – V2.1.1
ETSI GR ENI 007	Experiential Networked Intelligence (ENI); ENI Definition of Categories for AI Application to Networks – V1.1.1
ETSI GR ZSM 004	Zero-touch network and Service Management (ZSM); Landscape – V1.1.1
ETSI GS ENI 001	Experiential Networked Intelligence (ENI); ENI use cases – V2.1.1
ETSI GS ENI 002	Experiential Networked Intelligence (ENI); ENI requirements – V2.1.1
ETSI GS ENI 005	Experiential Networked Intelligence (ENI); System Architecture – V1.1.1
ETSI GS MEC 002	Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements – V2.1.1
ETSI GS ZSM 001	Zero-touch network and Service Management (ZSM); Requirements based on documented scenarios – V1.1.1
ETSI GS ZSM 002	Zero-touch network and Service Management (ZSM); Reference Architecture – V1.1.1
ETSI GS ZSM 007	Zero-touch network and Service Management (ZSM); Terminology for concepts in ZSM – V1.1.1
ETSI SR 003 680	SmartM2M; Guidelines for Security, Privacy and Interoperability in IoT System Definition; A Concrete Approach – V1.1.1
ETSI TR 102 647	Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Management; Operation Support System Standards Overview and Gap Analysis – V1.2.1; Includes Diskette
ETSI TR 102 659-1	GRID; Study of ICT Grid interoperability gaps; Part 1: Inventory of ICT Stakeholders – V1.2.1
ETSI TR 103 077	Universal Communications Identifier (UCI); Maximizing the Usability of UCI Based Systems – V1.1.1
ETSI TR 103 306	CYBER; Global Cyber Security Ecosystem – V1.4.1
ETSI TR 103 438	User Group; User centric approach in Digital Ecosystem – V1.1.1; Includes Diskette
ETSI TR 103 508	SmartM2M; SAREF extension investigation; Requirements for Automotive – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 536	SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms – V1.1.2
ETSI TR 103 562	Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2 – V2.1.1
ETSI TR 103 582	EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations – V1.1.1
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
ETSI TR 103 626	Autonomic network engineering for the self-managing Future Internet (AFI); An Instantiation and Implementation of the Generic Autonomic Network Architecture (GANA) Model onto Heterogeneous Wireless Access Technologies using Cognitive Algorithms – V1.1.1
ETSI TR 103 644	CYBER; Increasing smart meter security – V1.1.1
ETSI TS 103 195-2	Autonomic network engineering for the self-managing Future Internet (AFI); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management – V1.1.1

ETSI TS 103 300-2	Intelligent Transport System (ITS); Vulnerable Road Users (VRU) awareness; Part 2: Functional Architecture and Requirements definition – V2.1.1; Release 2
ETSI TS 105 174-8	Access, Terminals, Transmission and Multiplexing (ATTM); Broadband Deployment and Lifecycle Resource Management; Part 8: Implementation of WEEE practices for ICT equipment during maintenance and at end-of-life – V1.2.1
IEC 60050-171	International Electrotechnical Vocabulary (IEV) – Part 171: Digital technology – Fundamental concepts – Edition 1.0
IEC 60194	Printed board design, manufacture and assembly – Terms and definitions
IEC 61508 SET REDLINE	Functional Safety of Electrical/Electronic/programmable Electronic Safety – Related Systems Set *** Contains IEC 61508-1 Through IEC 61508-7*** – Edition 2.0; ***NOT AVAILABLE FOR CUSTOM COLLECTIONS AT THIS TIME*** All Retail Customer Must Purchase the DVD
IEC 61508-7	Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 7: Overview of techniques and measures – Edition 2.0
IEC 62243	Artificial intelligence exchange and service tie to all test environments (AI-ESTATE)
IEEE 1484.1	IEEE Standard for Learning TechnologyLearning Technology Systems Architecture (LTSA) – IEEE Computer Society
IEEE 1636	Software Interface for Maintenance Information Collection and Analysis (SIMICA)
IEEE 1671.1	Automatic Test Markup Language (ATML) Test Descriptions
IEEE 1900 SERIES	Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management – Includes IEEE 1900.1, IEEE 1900.2, IEEE 1900.4, IEEE 1900.4a, IEEE 1900.4.1, IEEE 1900.5, IEEE 1900.5.2, IEEE 1900.6, IEEE 1900.6A, IEEE 1900.7
IEEE 1900.1	Definitions and Concepts for Dynamic Spectrum Access: Terminology Relating to Emerging Wireless Networks, System Functionality, and Spectrum Management
IEEE 1934	Adoption of OpenFog Reference Architecture for Fog Computing
IEEE 2413	An Architectural Framework for the Internet of Things (IOT) – IEEE Computer Society
IEEE 2430	Trial-Use Standard for Software Non-Functional Sizing Measurements – IEEE Computer Society
IEEE 24765	Systems and software engineering – Vocabulary – IEEE Computer Society
IEEE 2755.1	Guide for Taxonomy for Intelligent Process Automation Product Features and Functionality
IEEE 7010	Recommended Practice for Assessing the Impact of Autonomous and Intelligent Systems on Human Well-Being
IEEE 802.22	Information Technology – Telecommunications and information exchange between systems Wireless Regional Area Networks (WRAN) – Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the Bands that Allow Spectrum Sharing where the Communications Devices May Opportunistically Operate in the Spectrum of Primary Service – IEEE Computer Society
IEEE NEUROTECHNOLOGIES BMI ROADMAP	STANDARDS ROADMAP: NEUROTECHNOLOGIES FOR BRAIN-MACHINE INTERFACING
IEEE WHITE PAPER 3DBP IC	IEEE 3D BODY PROCESSING INDUSTRY CONNECTIONS (3DBP IC): COMMUNICATION, SECURITY, AND PRIVACY
IEEE WHITE PAPER-0	Pre-Standards Workstream Report: Clinical IoT Data Validation and Interoperability with Blockchain
ISO 16355-3	Applications of statistical and related methods to new technology and product development process Part 3: Quantitative approaches for the acquisition of voice of customer and voice of stakeholder
ISO 24617-1	Language resource management – Semantic annotation framework (SemAF) – Part 1: Time and events (SemAF-Time, ISO-TimeML)
ISO 24617-7	Language resource management – Semantic annotation framework Part 7: Spatial information
ISO 9409-1	Manipulating industrial robots – Mechanical interfaces – Part 1: Plates
ISO IWA 31	Risk management – Guidelines on using ISO 31000 in management systems
ISO TR 23455	Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems – First edition

ISO/IEC 11179-1	Information technology – Specification and standardization of data elements – Part 1: Framework for the specification and standardization of data elements
ISO/IEC 19788-3	Information technology – Learning, education and training – Metadata for learning resources – Part 3: Basic application profile AMENDMENT 1
ISO/IEC 20748.4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/IEC 23001-4	Information technology – MPEG systems technologies – Part 4: Codec configuration representation
ISO/IEC 2382-1	Information technology – Vocabulary – Part 1: Fundamental terms
ISO/IEC 27021	Information technology – Security techniques – Competence requirements for information security management systems professionals
ISO/IEC TR 23188	Information technology – Cloud computing – Edge computing landscape
ISO/IEC TR 24741	Information technology – Technical Report for a Biometrics Tutorial (Technical Report)
ISO/IEC TR 27550	Information technology – Security techniques – Privacy engineering for system life cycle processes – First edition
ISO/IEC TS 20748-4	Information technology for learning, education and training – Learning analytics interoperability Part 4: Privacy and data protection policies
ISO/TR 23455	Blockchain and distributed ledger technologies – Overview of and interactions between smart contracts in blockchain and distributed ledger technology systems
ISO/TR 23845	Biomimetics – Ontology-Enhanced Thesaurus (OET) for biomimetics
ISO/TS 22287	Health informatics – Workforce roles and capabilities for terminology and terminology services in healthcare (term workforce)
ITU-T F.749.10	Requirements for communication services of civilian unmanned aerial vehicles – Study Group 16
ITU-T L.1022	Circular economy: Definitions and concepts for material efficiency for information and communication technology – Study Group 5
ITU-T L.1305	Data centre infrastructure management system based on big data and artificial intelligence technology – Study Group 5
ITU-T L.1380	Smart energy solution for telecom sites – Study Group 5
ITU-T M.3041	Framework of smart operation, management and maintenance – Study Group 2
ITU-T Q.1200	General Series Intelligent Network Recommendation Structure – Series Q: Switching and Signalling – Intelligent Network – Study Group 11; 11 pp
ITU-T SERIES K SUPP 16	Electromagnetic field compliance assessments for 5G wireless networks – Study Group 5
ITU-T Y.3101	Requirements of the IMT-2020 network – Study Group 13
ITU-T Y.3173	Framework for evaluating intelligence levels of future networks including IMT-2020 – Study Group 13
ITU-T Y.3324	Requirements and architectural framework for autonomic management and control of IMT-2020 networks – Study Group 13
ITU-T Y.3508	Cloud computing – Overview and high-level requirements of distributed cloud – Study Group 13
ITU-T Y.3800	Overview on networks supporting quantum key distribution – Study Group 13
ITU-T Y.4003	Overview of smart manufacturing in the context of the industrial Internet of things – Study Group 20
ITU-T Y.4204	Accessibility requirements for the Internet of things applications and services – Study Group TSAG
ITU-T Y.4904	Smart sustainable cities maturity model – Study Group 20
ITU-T Y.4906	Assessment framework for digital transformation of sectors in smart cities – Study Group 20
NEMA IOT P2	A NEMA White Paper on Emerging Technologies and the Industrial Internet of Things and Their Applications
SAE AIR1266A	Fault Isolation in Environmental Control Systems of Commercial Transports
SAE ARP5150A	(R) Safety Assessment of Transport Airplanes in Commercial Service
SAE ARP6407	IVHM Design Guidelines

SAE PT-202	Material and Process Modeling of Aerospace Composites – To Purchase Call 1-800-854-7179 USA/ Canada or 303-397-7956 Worldwide
SAE PT-204	Multi-Agent Safety: Book 2 – Automated Vehicle Safety – To Purchase Call 1-800-854-7179 USA/ Canada or 303-397-7956 Worldwide
SAE PT-205	Safety of the Intended Functionality: Book 3 – Automated Vehicle Safety – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SAE PT-207	The Safety of Controllers, Sensors, and Actuators: Book 5 – Automated Vehicle Safety – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SAE R-441	No Fault Found: The Search for the Root Cause – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
SAE R-463	Introduction to Advanced Manufacturing – To Purchase Call 1-800-854-7179 USA/Canada or 303-397-7956 Worldwide
UL 4600	UL STANDARD FOR SAFETY Evaluation of Autonomous Products – First Edition

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

IMDRF/SaMD WG/ N10FINAL:201	Software as a Medical Device (SaMD): Key Definitions (IMDRF/SaMD WG/N10FINAL:2013)
IMDRF/SaMD WG/ N12FINAL:2014	Software as a Medical Device (SaMD): Possible Framework for Risk Categorization and Corresponding Considerations (IMDRF/SaMD WG/N12FINAL:2014)
IMDRF/SaMD WG/N23 FINAL:2015	Software as a Medical Device (SaMD): Application of Quality Management System (IMDRF/SaMD WG/ N23 FINAL:2015)
N/A	Guidance Document: Software as a Medical Device (SaMD): Definition and Classification
N/A	Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) – Discussion Paper and Request for Feedback
ISO/IEC DTR 29119-11	Software and systems engineering – Software testing – Part 11: Testing of AI-based systems
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
CAN/CIOSC 107	Testing and proving grounds for autonomous vehicles
IEEE P1232.3/D3.2	IEEE Approved Draft Guide for the Use of Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE)

Issue 31 — Data value chain

ETSI TR 103 376	SmartM2M; IoT LSP use cases and standards gaps – V1.1.1
ITU-T Y.3601	Big data – Framework and requirements for data exchange – Study Group 13
ETSI TR 103 305-5	CYBER; Critical Security Controls for Effective Cyber Defence; Part 5: Privacy enhancement – V1.1.1
ETSI TR 103 534-2	SmartM2M; Teaching material; Part 2: Privacy – V1.1.1; Includes Diskette
ETSI TR 103 603	User Group; User Centric Approach; Guidance for providers and standardization makers – V1.1.1
IEEE 1232.1	Trial Use – Standard for Artificial Intelligence Exchange and Service Tie to All Test Environments (AI-ESTATE): Data and Knowledge Specification

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

N/A	Realising the value of health care data: a framework for the future
N/A	Study: The value of data in Canada: Experimental estimates

N/A	Competence Center Corporate Data Quality (CC CDQ)
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
IEEE IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

Issue 32 —
Transparency and communication of data analytics

ISO/IEC TR 24028	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

n/a	Datasheets for Datasets
n/a	Public Opinion Research Standards and Disclosure Requirements
n/a	A privacy-preserving data cloud for health care
ISO/IEC 20889:2018	Privacy enhancing data de-identification terminology and classification of techniques
n/a	The value of a shared understanding of AI models
n/a	Explainable Artificial Intelligence (XAI)
n/a	Regulation (EU) 2016/679 of the European Parliament and the Council – on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
n/a	Algorithmic Impact Assessment (AIA)
n/a	Open Data
n/a	Designing for Digital Transparency in the Public Realm
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-1:2020	Data governance – Part 1: Data protection of digital assets
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-8	Data Governance – Part 8: Framework for Geo-Residency and Sovereignty
IEEE P7001	IEEE Draft Standard for Transparency of Autonomous Systems
IEEE IC18-004	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

Issue 33 —
Interpretability and explainability of AI systems (Originally “Interpretability of algorithms.)

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

n/a	Explainable Artificial Intelligence (XAI)
n/a	Ethics Guidelines for Trustworthy AI

n/a	Regulation (EU) 2016/679 of the European Parliament and the Council – on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
ISO/IEC DTR 29119-11	Software and systems engineering – Software testing – Part 11: Testing of AI-based systems
n/a	White Paper on Artificial Intelligence – A European approach to excellence and trust
ISO/IEC TR 24028:2020	Information technology – Artificial intelligence – Overview of trustworthiness in artificial intelligence
n/a	Data Ethics Canvas
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
IEEE P2894	Guide for an Architectural Framework for Explainable Artificial Intelligence

Issue 34 —
Assessment and management of bias

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

ISO/IEC AWI TR 24027	Information technology – Artificial Intelligence (AI) – Bias in AI systems and AI aided decision making
IEEE P7003	Algorithmic Bias Considerations
n/a	Ethical Guidelines for Statistical Practice
n/a	The Data Equity Framework
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada
CAN/CIOSC 100-3	Data governance – Part 3: Privacy enhancing data de-identification framework
CAN/CIOSC 100-6	Data governance – Part 6: Responsible collection and use of digital contact tracing and monitoring data in the workplace
CAN/CIOSC 100-7	Data Governance – Part 7: Operating model for responsible data stewardship
CAN/CIOSC 101:2019	Ethical design and use of automated decision systems
IEEE P7003	Algorithmic Bias
N/A	Ethics Certification Program for Autonomous and Intelligent Systems (ECPAIS)

Issue 35 —
Performance management systems for analytics and AI systems

OTHER GUIDANCE/DOCUMENTS/STANDARDS PROPOSED BY WORKING GROUP MEMBERS

ISO/IEC 38507	Information technology – Governance of IT – Governance implications of the use of artificial intelligence by organizations
n/a	Ethical Dimensions of Using Artificial Intelligence in Health Care
n/a	ISO MANAGEMENT SYSTEM STANDARDS (MSS)
CAN/CIOSC 100-n	Series of standards for data governance
CAN/CIOSC 100-5	Data governance – Part 5: Health data and information capability framework
CAN/CIOSC 111-x	Series of standards supporting the implementation of online electoral voting in Canada

Annex C —

Indigenous Engagement on the DGSC

Indigenous Engagement on the Data Governance Standardization Collaborative – Initial Perspectives on Data Governance Issues

Thanks and acknowledgements go to survey respondents and interview participants for sharing their input, guidance and perspectives on data governance. This engagement report could not have been completed without their support and expert knowledge.

Indigenous Data Sovereignty

It is important to contextualise use of the term Indigenous Data Sovereignty within this report at the outset. In the Canadian context, the term Indigenous refers to First Nations, Inuit and Métis. It is essential to acknowledge that data sovereignty is not a pan-Indigenous exercise where one approach is adopted by all but rather one that is defined and led by First Nations, Inuit and Métis. In using the term Indigenous Data Sovereignty in this report, we refer to the collective efforts of First Nations, Inuit and Métis to achieving data sovereignty in a manner that is in keeping with their unique laws, cultures, protocols, and worldviews.

Prepared and authored by:
Firelight Research Inc.

the
firelight
group

Table of contents

Executive Summary

The Standards Council of Canada retained Firelight to support the design, development, administration, virtual logistics, and facilitation of initial Indigenous engagement across Canada. The objective of this initial engagement is to add Indigenous perspectives on data governance in Canada into considerations for the Data Governance Standardization Collaborative (DGSC) roadmap. Engagement activities included an online survey and key participant interviews. This report provides background on issues related to Indigenous data governance and sovereignty, summarises the results of engagements, and provides a number of recommendations based on input provided by participants. Participants gave consent to use their input in this report prior to survey or interview completion.

Indigenous Peoples (i.e., First Nations, Inuit, and Métis, within the Canadian context), like all populations, require high quality data about citizens, communities, lands, resources, and culture to support evidence-based decision-making. Yet Indigenous Peoples and their governing bodies continue to struggle to gain autonomy over data governance activities. Historically and currently, the collection and management of data about Indigenous communities is largely administered by external bodies; lacking Indigenous leadership, and not reflective of the priorities, needs, worldviews, and values of Indigenous communities. This has led to the extraction of data from communities, use of inappropriate indicators to measure health and well-being, and misuse of data about Indigenous peoples. It is within this context that Indigenous data sovereignty is emerging — the right of an Indigenous governing body to govern the collection, ownership, dissemination, and application of its own data about its communities, members, lands, and resources. Indigenous data represents a significant feature of Indigenous sovereignty as a whole, and a movement toward self-governance, self-determination, and decolonization.

An online survey was selected as a means of engagement in order to reach as broad a group as possible within the engagement timeline. The online survey sought input from participants on the nature and importance of the ten issues identified by Working Group 1 within an Indigenous context. The online survey was launched, in both English and French, on January 12th, 2021 and was closed on February 2nd, 2021. A total of 36 people completed the English language version of the survey. There were no completions of the French language survey. Participants were asked to rate the importance of each of the ten Foundations of Data Governance issues. *Guidance on Trustworthiness, Ethical, and Societal Use of Data*; *Accountability Frameworks*; and *Data Management Governance* were most frequently ranked by participants as being *very important* issues to focus on when developing data governance standards. None of the issues were ranked as not important. Results of the survey are outlined in Section 4.1. Further input provided by survey participants on each issue is summarised in Table 3 below.

Key participant interviews took place with practitioners and experts in First Nations, Inuit, or Métis data governance data governance in order to gain a more in-depth understanding of Indigenous perspectives on these issues. Interview participants were identified based on their expertise and experience working with organisations and/or on projects and initiatives that focus on Indigenous data governance issues. Firelight endeavoured to interview key participants from across Canada with expertise across the unique data governance landscapes of First Nations, Inuit, and Métis communities. Approximately half of those invited to complete an interview were able or willing to participate. A total of 12 interviewees contributed as part of 8 key participant interviews. Section 3.3 provides an overview of key interview participants.

A number of key Indigenous data governance issues were identified upon thematic analysis of survey and interview responses:

- Recognition of Authority: The lack of recognition of the authority of Indigenous governments as sovereign decision-makers over all aspects of the life cycle of data relating to their populations, lands and waters.
- Capacity: The capacity of Indigenous governments and organisations to govern the collection, management, storage, and sharing of data. Capacity was described in terms of infrastructure, equipment, human resources, training, technology, and funding.
- Access to Data: Indigenous governments and organisations often do not have access to necessary information about the populations they serve and the lands and waters they administer. With information housed by researchers, government, and other organisations, Indigenous decision-makers lack the necessary information to govern.
- Culturally Appropriate Data: Data collection needs to be led by Indigenous organisations, and data collection and management methods need to be reflective of the unique Indigenous cultural context, values, and norms relevant to each undertaking.

This report can be used as an initial account of perspectives on Indigenous data governance issues as well as potential means to tackle these issues, but there are a number of limitations to the report that require consideration in interpreting the results. A limited number of participants from Inuit and Métis organisations contributed to the engagements conducted. Due to limitations of time and budget, detailed engagement on each of the 35 issues identified by the DGSC working groups was not possible. The limitations of this report are discussed further in Section 1.3.

A number of existing principles, standards, and initiatives were highlighted by participants that are of direct relevance to the potential development of data governance standards. These initiatives all assert the sovereignty of Indigenous Peoples to control all aspects of the collection, management, and use of data. These are profiled in Section 4.3 and include the First Nations Principles of OCAP®, the First Nations Data Governance Strategy (FNDGS), and the National Inuit Strategy on Research (NISR).

A number of recommendations are provided in Section 5 below based on the input provided during engagements and relating to the continued engagement and participation of Indigenous governments and organizations in the DGSC process.

1. Additional engagement of Inuit and Métis organisations and data governance experts is required. Due to limited participation of Inuit and Métis practitioners and experts in engagements, further work is required in order to capture the perspectives of these key Indigenous groups on data governance issues and on the work of the DGSC.
2. Further involvement of Indigenous governments and organizations in the DGSC process will be necessary in order to dedicate the time and resources necessary to clearly defining issues brought forward by Indigenous governments and organizations and integrating them, where appropriate, into issues already defined by DGSC working groups. This may also include participation of Indigenous representatives in DGSC working groups. For example, based on their high ranking in survey results, a number of key issues from Working Group 1, including *Guidance on Trustworthiness, Ethical, and Societal use of Data, Accountability Framework*, and *Data Management Governance* will require further input from Indigenous governments and organizations.
3. Identifying key Indigenous organisations (including those already developing standards or principles such as Inuit Tapiriit Kanatami and the First Nations Information Governance Centre) to participate in further phases of DGSC work, including standards development, will be a necessary outcome of further engagements.

1. Introduction

1.1 OVERVIEW

This summary report provides results from initial Indigenous engagement on data governance issues conducted for the Data Governance Standardization Collaborative. It should be noted at the outset that this report and its contents do not provide the sum of Indigenous perspectives on data governance, nor does it purport to represent all First Nations, Inuit and Métis perspectives. Further details on the limitations of the engagements carried out and information collected during them is described in Section 1.3 below. Continued engagement of Indigenous governments and organizations in the DGSC process will be required in order to allow Indigenous participation and leadership in developing and enforcing any standards or initiatives potentially resulting from the DGSC process.

Data governance has unique and distinct importance for First Nations, Inuit, and Métis communities collectively and individually. In order to provide important context to the input and feedback collected during initial Indigenous engagements, Section 2 of this report provides an overview of why Indigenous data governance is unique and tied to historical and ongoing impacts from colonization. This leads into a brief discussion of how Indigenous processes of decolonization and self-determination are fueling the data sovereignty movement. A summary of the engagement methods utilised is provided in Section 3. Results, including descriptions of the main issues brought forward during the course of engagements, are provided in Section 4. A number of recommendations based on input provided during engagement sessions are provided in Section 5.

1.2 SCOPE OF WORK

The Standards Council of Canada retained Firelight to support the design, development, administration, virtual logistics, and facilitation of initial Indigenous engagement across Canada. The objective of this initial engagement is to add Indigenous perspectives on data governance in Canada into considerations for the DGSC roadmap.

The main activities Firelight was engaged to perform include:

- Project initiation to develop a project plan and budget based on the scope of work and project goals;
- Design engagement in collaboration with SCC, including identification of appropriate methods for engagement, identification of appropriate participants using a suitable approach, and the development of questions and support materials to be used during engagement;
- Contacting key participants and scheduling interviews, managing virtual logistics and administration of engagements;
- Engaging with key stakeholders in structured discussions via a survey and one-one-one interviews with key participants; and
- Developing an overarching 15-30 page summary report (this report) outlining the engagements carried out and level of participation, as well as detailing the feedback heard throughout engagement.

The final engagement report (i.e., this Report), should capture the lessons learned and key insights of the Indigenous perspectives on data governance and should:

- Draw directly from current and ongoing research, knowledge, and best practices for Indigenous data sovereignty;
- Outline the tools and processes necessary to record and validate key physical data to support Indigenous data governance frameworks, where possible;
- Reflect guidance and knowledge gathered through engagement with First Nations, Inuit, and Métis knowledge holders, community-based data governance practitioners, and representative Indigenous organizations; and
- Respect First Nations, Inuit, and Métis guidelines for data collection, ownership, storage, and dissemination.

1.3 LIMITATIONS

The information contained within this report is based on feedback provided during a limited number of initial engagements with Indigenous groups and is subject to a number of limitations, including the following:

- Due to limitations of time and budget, detailed engagement on each of the 35 issues identified by the DGSC working groups was not possible. Survey questions focused on Working Group 1's Foundations of Data Governance issues, and interviews focused on the main data governance issues highlighted by key participants.
- Eight from a total of sixteen invitees contacted were unable to participate in an interview for a variety of reasons. Reasons given for not participating included lack of time and an invitee declining to share knowledge with researchers, while other invitees did not respond to an invitation to participate.
- While this summary report is based on engagement with Indigenous governments and organizations, the contents of this report should not be in any way construed or interpreted to represent a pan-Indigenous perspective on data governance issues. As highlighted by participants throughout, issues, priorities, and perspectives vary both across and within First Nations, Inuit, and Métis groups, as well as between regions and jurisdictions in Canada.
- In particular, a limited number of participants from Inuit and Métis organisations contributed to the engagements conducted. None of the key participants contacted from national or regional Métis organisations were able to participate in interviews. One interview participant works for an Inuit organization. *This is a key limitation of this report, as further detail on Inuit and Métis perspectives on data governance issues is required.*
- Engagement materials, along with the survey, were provided only in English and French due to time and budget limitations. Interviews were conducted in English and French. Additional detailed information could be collected through holding engagement in Indigenous languages, due to the importance of Indigenous languages as unique means of communicating culture and ways of knowing and being.

Given the above limitations, this report can be used as an initial account of perspectives on Indigenous data governance issues as well as potential means to tackle these issues. Further engagement is necessary in order to identify and clearly define further issues and identify how Indigenous perspectives can contribute to addressing issues, including through the potential development of standards.

2. Data Governance and Indigenous Communities

Data sovereignty has emerged as an important topic, raising fundamental questions about the inherent right of a sovereign body to collect, control, and manage its own data (Snipp 2016, 39). Indigenous Peoples, like all populations, require high quality data about citizens, communities, lands, resources, and culture to support evidence-based decision-making.[18] Yet Indigenous Peoples and their governing bodies continue to struggle to gain autonomy over data governance activities. In many ways, data collection activities regarding Indigenous Peoples remain both a political and logistical exercise administered by colonial governments. This causes data collection to continually reiterate and reinforce colonial structures designed to administrate Indigenous Peoples, land, and resources.

As the scale and scope of Indigenous Peoples' economic, social, and cultural development accelerates, the demand for Indigenous data is increasing. The increased proliferation of data has given rise to Indigenous data sovereignty – the right of an Indigenous governing body to govern the collection, ownership, dissemination, and application of its own data about its communities, members, lands, and resources. Indigenous Peoples have increasingly recognized the importance of asserting sovereignty and establishing comprehensive governance processes to decolonize data. Indigenous Peoples now have the opportunity to use data to meet their own needs and priorities. It is in this context whereby Indigenous Peoples are challenging dominant discourses through data that is developed by and for communities, reflects Indigenous worldviews, and that is culturally appropriate and sensitive. Data, when developed, gathered, and used correctly, provides Indigenous Peoples with a way to bring evidence to issues that are often ignored.

2.1 INDIGENOUS DATA CHALLENGES

The following outlines some of the issues that underpin the wider Indigenous data sovereignty movement. These issues reveal the historical and contemporary critical vestiges of how non-Indigenous-led data collection and management practices impact Indigenous Peoples.

2.1.1 Colonial Context of Data Collection and Use

The Indigenous data sovereignty landscape must be positioned within the historical and contemporary arenas of colonisation. Contemporary policy-making and decision-making is increasingly rooted in state-driven data collection initiatives (McMahon et al. 2017, 432).

Historically, data collection activities pertaining to Indigenous populations were largely driven by federal and provincial agencies, universities, and other external actors, often justifying and sustaining existing structures to operationalize government policies on control, surveillance, and assimilation over Indigenous Peoples. Data collection was operationalized through quantitative datasets and indicators that reflected western preoccupations and values to supplant Indigenous economies, erode customary laws, protocols, and knowledge systems, undermine Indigenous leadership, enumerate Indigenous Peoples into populations, and appropriate Indigenous land and resources (Smith 2016, 117-135). For example, state-driven data collection activities pathologized Indigenous social, economic, and political institutions to buttress and rationalize the violent assimilation of Indigenous Peoples into settler society through colonial structures, such as residential schools and the '60s Scoop (TRC 2015). As noted by Raine et al. (2019, 304), data on Indigenous Peoples often perpetuates "a narrative of inequality, creating a dominant portrait of Indigenous Peoples as defined by their statistically measured disparity, deprivation, disadvantage, dysfunction, and difference."

[18] Indigenous data encompasses an amalgamation of data, information, and knowledge about Indigenous individuals, collectives, communities, cultures, knowledge, science, ceremonies, lands, and resources.

Currently, the collection of Indigenous data remains primarily viewed as servicing external interests rather than supporting Indigenous needs and priorities, and can undermine Indigenous sovereignty and self-determination. Thus, the inherently political natural of data collection and persistent structural colonization through data practices facilitates a landscape of mistrust where Indigenous Peoples resist sharing information (RCAP 1996).

2.1.2 Data Extraction and Exclusion

Stemming from a lack of respectful relationships between those collecting data and Indigenous Peoples, Indigenous data has historically been extracted from communities in a manner whereby Indigenous Peoples and governing bodies are excluded from expressing autonomy over the data collected about them. Particularly, external agents such as academic institutions and government agencies have often excluded Indigenous Peoples from the interpretations and presentations of research findings derived from the data collected on them (McBride 2018, 6). This exclusion has often resulted in the harmful misinterpretation of Indigenous data and even the pathologizing of Indigenous Peoples (McBride 2018, 6), such as in the case of the Nuu-chah-nulth Nation in British Columbia.

In this case, a University of British Columbia professor collected over 800 blood samples originally to preform research on the increased presence of arthritis in the Nuu-chah-nulth Nation. Without any form of engagement with the Nuu-chah-nulth, the professor later used the blood samples to produce over 200 research reports unrelated to the original arthritis study. The subject areas of these reports included research into HIV/AIDS and theories about migration patterns that completely undermined the Nuu-chah-nulth traditional beliefs on Creation (FNIGC 2016, 145).

The historic and contemporary exclusion of Indigenous Nations from practicing autonomy over data on them has further perpetuated the mistrust that Indigenous Peoples carry towards data collection activities in general. Demonstrated in the Nuu-chah-nulth case, data is often used in ways that Indigenous Nations do not support and often in a manner that does not respect commitments initially set out prior to the commencement of the research (Raine et al. 2017, 4). As reiterated by Steffler (2016, 151), "[t]his approach has created a situation in which there is a lack of trust, 'buy-in,' and participation on the part of Indigenous communities – inevitably affecting the overall quality of the data." Consequently, western academic data collection practices continue to have residual effects that maintain an enduring climate of distrust and suspicion, and resistance to disclosing information between Indigenous Peoples and external actors.

2.1.3 Research does not Reflect Indigenous Needs and Priorities

The collection, management, and dissemination of Indigenous data has been historically generated without Indigenous participation and/or informed consent. As a result, most data collected about Indigenous Peoples remains irrelevant and inaccurate, articulated through a settler colonial lens. As noted by the 1996 *Report of the Royal Commission on Aboriginal Peoples* (RCAP), data about Indigenous Peoples remains observed as serving external interests due in large part to the complex ongoing impacts of settler colonialism.[19]

[19] "The gathering of information and its subsequent use are inherently political. In the past, Aboriginal people have not been consulted about what information should be collected, who should gather that information, who should maintain it, and who should have access to it. The information gathered may or may not have been relevant to the questions, priorities and concerns of Aboriginal peoples. Because data gathering has frequently been imposed by outside authorities, it has met with resistance in many quarters (Government of Canada 1996, p. 4)."

Thus, it is important to note that Indigenous Peoples have been researched to death, persistently targeted by state-driven data collection that primarily benefits external entities, such as governments, corporations, or research institutions. Through the imposition of western data collection practices, Indigenous Peoples are denied meaningful involvement through external data collection efforts, where external entities present "completed research designs, often already funded, for community approval rather than collaboration from the start" (FNGIC 2016, 143). Often, such data collection initiatives pre-empt meaningful engagement and informed consent with Indigenous Peoples, whereby Indigenous data is subject to exploitation and misinterpretation. As a result, data collection activities fail to reflect Indigenous aspirations and needs.

In many cases, state-driven data collection processes are motivated by federal and provincial administrations that define the research metrics and measurements. The majority of research conducted on Indigenous Peoples pathologizes Indigenous communities, focusing on chronic health issues, such as diabetes, alcoholism, and suicide (FNIGC 2014). While important, these studies reduce Indigenous lived experiences to statistical data, failing to address the consequences of colonisation, such as intergenerational trauma, systemic racism, and gender-based violence (FNIGC 2014; Dewar 2019, 4).

2.2 INDIGENOUS DATA SOVEREIGNTY AND GOVERNANCE: OWNERSHIP, CONTROL, AND REPRESENTATION

2.2.1 Indigenous Data Sovereignty

Data sovereignty is a uniquely twenty-first-century construct that is directly correlated to the rapid development, transformation, and accessibility of data. Data sovereignty refers to the concept that data is subject to the laws and governance structures within which it is located.

Indigenous data sovereignty emerged as a response to the historic and contemporary role of knowledge production to reproduce colonial relationships between Indigenous governments and organisations and the Government of Canada (Espey 2002). The Indigenous data sovereignty landscape gives rise to a wide-ranging set of legal, ethical, and practical considerations. Indigenous data sovereignty asserts the rights of Indigenous Peoples to govern the collection, dissemination, ownership, and administration of their own data (Kukutai and Taylor 2016). This assertion is derived from a sovereign body's right to govern their peoples, lands, and resources. Stemming from the shift to decolonize data, the emergences of Indigenous data sovereignty practices can be observed through a variety of Indigenous governance models.

Indigenous data sovereignty is highlighted by the following principles:

1. Indigenous governing body's data includes any facts, knowledge, and/or information about its people, communities, land, and resources.
2. Research and data collection activities reflect the needs and priorities of an Indigenous Nation.
3. Indigenous Peoples are meaningfully involved and consulted in all aspects of the research process.
4. Research must include culturally appropriate and sensitive processes that reflect Indigenous worldview, values, ethics, and protocols.
5. Indigenous governing bodies have the jurisdiction over the collection, ownership, and application of its data.
6. Data remains subject to an Indigenous community's traditional laws and protocols.

Indigenous data collection, analysis, and stewardship, designed by Indigenous Peoples for Indigenous Peoples, provide an invaluable resource for autonomy, development, and aspirations for Indigenous Peoples. In other words, Indigenous data represents a significant feature of Indigenous sovereignty, and movement toward self-governance, self-determination, and decolonization.

2.2.2 Indigenous Data Governance

Linked to the concept of Indigenous data sovereignty is Indigenous data governance. Indigenous data governance provides the mechanisms to enact the inherent right of Indigenous Peoples to control the collection, dissemination, management, and application of their own data. Indigenous Peoples, whose traditional knowledge systems have often been disrupted and assimilated by Western colonial data practices, are reasserting autonomy through Indigenous data governance mechanisms (Lovett et al. 2019).

Indigenous data governance is highlighted by the following principles:

1. Indigenous governing bodies obtain the decision-making authority to assign the duties and responsibilities pertaining to the management of all data about them.
2. Indigenous governing bodies obtain the decision-making authority on the design, interpretation, validation, ownership, access to, and use of all data relating to them.
3. Indigenous governing bodies obtain the decision-making authority to establish their own culturally-appropriate measures and definitions which are used in the processes of data production, ownership, analysis, and administration.

Indigenous data governance is the guiding framework of data governance that allows for Indigenous data sovereignty to be achieved. Examples of prominent Indigenous data governance initiatives are provided below in Section 4. The initiatives described provide the mechanisms necessary to achieving Indigenous data sovereignty for the groups leading them through asserting ownership, control, and representation over the collection, dissemination, and administration of their own data.

3. Methods

Engagement methods included an online survey and interviews with key participants. The methods utilised for both engagement activities are described below, including selection of participants, documentation of informed consent, and methods of analysis.

3.1 INFORMED CONSENT AND MANAGEMENT OF COLLECTED DATA

All participants provided informed consent prior to participating in the survey or key participant interviews. Consent forms for both the survey and interviews describe the goals and process of the engagement and wider DGSC roadmap development and describe what information would be collected and how this information would be managed. See Appendix 1 for the Interview Consent Form and Appendix 2 for survey text, including consent page.

3.1.1 Surveys

A consent page was added to the survey, immediately following the introductory page. Following an explanation of the work and how information would be collected and managed, participants were provided with a Yes/No question that asked if they give consent to continue. If participants responded ‘No’ to this question, the survey ended, without any information being collected other than noting that a potential participant did not provide consent to continue. By answering ‘Yes’, participants were brought to the first question of the survey. Contact details for the team at Firelight were provided on the consent page in order to allow potential participants to directly reach out with questions on the engagement. Individuals participated in the survey anonymously and individual responses were considered confidential. Survey respondents were asked to not add any contact details or identifying information to their responses. An incentive was offered to survey participants in the form of the chance to win a $100 gift card – participants entered by filling out a separate survey form linked from the final page of the survey.

The data collected during the survey was stored on Survey Monkey servers until the survey closed on 2nd February 2021. The survey data was then transferred onto a secure Canada-based server owned by the Firelight Group, where it is currently stored. All survey data will be deleted from the server within one year of being collected.

3.1.2 Key Participant Interviews

For interviews, a consent form (see Appendix 1[20]) was reviewed with each participant prior to each interview starting. The consent form outlines the purpose of the interview, outlines how information collected would be used and stored, and asks a number of questions of participants regarding their participation in the interview.

As outlined in the consent form, key participants will maintain ownership over their responses. Following every interview, each participant was sent their interview transcript and recording. Each participant retains the rights to their respective interview transcript and recording. Zoom recordings of the interviews were initially saved locally on a laptop and then moved to a secure Canada-based server owned and operated by the Firelight Group. Copies of interview and data will be stored on this server until it is deleted, within one year of being collected.

The consent form also asks participants whether they agree to have quotes from their interview used in the report, how they would like their quotes to be attributed (if permission is given to use them) and whether they would like their names included in the report. For all of these questions, participants hold the rights to withdraw consent for use of their quotes or listing of their name in the report. Participants were each provided with a copy of the draft report and hold the right to make any changes to interpretations or quotes prior to the final draft of this report being assembled. Key participants were assigned a personal identification number (PIN) in the form of I## in order to maintain confidentiality. For participants who chose not to have their name attributed to quotes, their PIN was used in place of their name. For this reason, a mixture of names and PINs are used to attribute quotes throughout this report. Quotes, and attributions of quotes, are only used in this report with permission of the interviewee. Names are only included in this report with the permission of the interviewee.

Consent for key interviews was given by participants through two means. After reviewing and revising the consent form with Firelight staff, participants gave verbal consent to proceed with the interview at the outset of each recording. Hard copies of consent forms were also signed by participants and provided to Firelight. As each interview was conducted remotely, not all interviewees had access to a printer and scanner in order to sign and return a signed hard copy of the consent form. For these cases, consent was provided verbally only.

3.2 SURVEY

An online survey was selected as a means of engagement in order to reach as broad a group as possible within the engagement timeline. The goal of the survey is to gain an initial understanding of: what data governance issues are most important to Indigenous groups, what initiatives or standards exist to tackle these issues, and how respondents envision the future of Indigenous data governance. An online platform was chosen as the most accessible means of reaching as many respondents as possible during the pandemic.

[20] A number of participants requested alterations to the wording used in the consent form in order to clarify what information would be collected, who would own it, how it would be used and stored, and how interview participants would retain the right to withdraw consent for inclusion of their materials in this report. The consent form provided in Appendix 1 represents the most comprehensive and detailed account of how recorded information would be collected, owned, and stored as part of this engagement project.

Indigenous engagement was originally scoped to seek feedback on all 35 issues identified by the four DGSC Working Groups. During meetings between Firelight and SCC during the initiation and engagement design phases of work, it was determined that time and budget constraints of the engagements would not allow for sufficient depth of coverage on all issues. Additionally, it was determined that a survey seeking feedback from respondents on all 35 issues would be too onerous and lead to decreased rates of completion of the survey. For this reason, the survey questions focused on getting feedback from respondents on Working Group 1's Foundations of Data Governance issues, namely:

- Accountability Framework
- Certification for Professional Roles
- Digital Literacy
- Cybersecurity Protection
- Data Management Governance
- Data Privacy
- Guidance on Trustworthiness Ethical & Societal use of Data
- Harmonization & Interoperability of Data Practices/Open Data
- Data Actor and Data Transaction Roles
- Secondary Use of Data

A mixed-methods approach was taken, using both open and closed-ended questions in order to get a mixture of quantitative and more descriptive qualitative data. The online survey was designed and deployed on the Survey Monkey online platform. Two copies of the survey were deployed – one in English and another in French.

Survey respondents were reached through a number of engagement methods including sharing links to both survey copies through Firelight and SCC social media channels in both English and French (including Facebook, Twitter, Instagram, and LinkedIn) and through directly sharing links to the surveys to Firelight's networks by email. Links to the surveys were shared publicly to Firelight's networks via a series of a total of 18 posts on social media platforms between the dates of January 12th and 26th, 2021. A link to the surveys was also shared via a Mighty Networks platform with the Indigenous Mapping Collective – a group of over 650 practitioners working in the field of Indigenous mapping in Canada and abroad. Firelight staff also shared links to the survey with their networks via email. Engagement materials are attached here as Appendix 4.

The results of the survey, including quantitative and qualitative data, are integrated into Section 4 below. Section 4.1 also provides an overview of the results of engagement and outreach conducted in order to share the survey with Firelight's networks.

3.3 KEY PARTICIPANT INTERVIEWS

Key participant interviews took place with practitioners and experts in Indigenous data governance in order to gain a more in-depth understanding of Indigenous perspectives on data governance issues. Currently, the DGSC working groups do not include Indigenous representatives, meaning the identification and definition of data governance issues to date has not included Indigenous perspectives. Interviews therefore focused on the primary data governance issues brought forward by key participants, in order to provide the opportunity for experts in Indigenous data governance to begin the process of defining and framing issues in a manner that they deem appropriate and relevant to their work. Interview questions were posed at a high level (see interview guide in Appendix 3) and the interview followed a semi-structured format in order to allow participants to highlight the most important issues and initiatives tackling these issues from their perspective.

Key participants were identified based on their expertise and experience working with organisations and/or on projects and initiatives that focus on Indigenous data governance issues. Firelight endeavoured to contact key participants with expertise across the unique data governance landscapes of First Nations, Inuit, and Métis communities. Additionally, engaging with key participants from different regions of Canada and across multiple disciplines was prioritised. With this in mind, a review of existing Indigenous data governance and data sovereignty initiatives in Canada, as well as a review of relevant literature materials on Indigenous data governance and data sovereignty was conducted. From this review process, a list of various communities, networks, and organizations was generated. Within these communities, networks, and organizations, individuals that work particularly closely in the realms of Indigenous data governance and Indigenous data sovereignty were identified as potential key informants. Furthermore, key informants were identified through recommendations from SCC staff and from interviews with other key informants.

A total of 16 key participants were contacted by a combination of phone and email between January 18th and February 18th, 2021, and invited to participate in an interview. Of these 16 invitees, eight work with First Nations organisations, two work with national Inuit organisations, five work with Métis organisations or initiatives, and one invitee works with an organisation working with First Nations, Inuit, and Métis data. A total of eight invitees agreed to participate in an interview. Five invitees declined an interview, and three invitees did not respond to invitations or follow-up messages.

None of the key participants contacted from national or regional Métis organisations were able to participate in interviews or responded to the invitation. One invitee who declined referred a colleague to be interviewed in their stead. Other reasons for declining an interview included lack of time; as well, one invitee declined to share their knowledge with researchers. Another invitee noted that further preparation within their organisation would be necessary before they could participate in an interview. One invitee, while declining an invitation, noted that deeper engagement than a key participant interview and survey would be required in order to capture the depth of Indigenous input on data governance issues.

Two invitees requested that colleagues join them in their interview, resulting in 8 interviews being conducted with a total of 12 key participants. A total of ten key participants work with First Nations organisations, one participant works with an Inuit organisation, and one participant works with an organisation that works on governance of First Nations, Inuit, and Métis data. Table 1 provides an overview of key participants in interviews. Key participants chose if and how they wished to be represented in Table 1, therefore not all key participants are listed below.

Table 1: Key participants

Mindy Denny, Union of Nova Scotia Mi'kmaq
An Indigenous researcher at the University of Guelph
Samantha Michaels, Senior Policy Advisor, Pauktuutit Inuit Women of Canada
Staff member from the Commission de la santé et de services sociaux des Premières Nations du Québec et du Labrador (CSSSPNQL)
Gwen Phillips, Ktunaxa Nation, BC Data Governance Champion
Jullian MacLean, NWT SPOR Unit: Hotii ts'eeda
Aaron Franks, Senior Advisor, First Nations Information Governance Centre
Nancy Gros-Louis McHugh, Gestionnaire secteur de la recherche, Commission de la santé et de services sociaux des Premières Nations du Québec et du Labrador (CSSSPNQL).
Erin Corston, Senior Advisor, First Nations Information Governance Centre
Patrice Lacasse, Conseiller en Gouvernance, Commission de la santé et de services sociaux des Premières Nations du Québec et du Labrador (CSSSPNQL)
Council of Yukon First Nations Staff Member

Interviews all took place remotely via Zoom videoconferencing software. Two Firelight staff attended interviews – one interviewer and one note taker. Audio and video from interviews were recorded locally on Firelight researchers' laptops. Firelight researchers also took notes during interviews. Interviews were of between 30 and 70 minutes duration. Seven interviews were conducted in English, with one interview conducted predominantly in French. Audio from all interviews was transcribed and later analysed. Each interview participant was assigned a PIN in the form of I## in order to maintain confidentiality.

3.4 ANALYSIS

Transcripts from key participant interviews, along with qualitative data from open-ended survey questions, were reviewed and analysed for emergent themes. A number of emergent themes were based on issues that were highlighted as the most important by key participants. Additional themes included potential ways of addressing data governance issues and visions for the future of Indigenous data governance. Finally, the ten issues identified by DGSC Working Group 1 were added as themes to tables that were used to code qualitative data, in order to highlight any potential connections that exist between these issues and those raised by participants. An additional layer of organisation was added to coding tables by noting the region of Canada the participant works in, along with noting whether the participant works with a First Nations, Inuit, or Métis organisation. These fields were added in order to aid with identification of the unique nature of issues in different regional and cultural contexts.

4. Results

The Section gives an overview of the results of the engagement. Section 4.1 provides an overview of the results of the online survey. Following this, Section 4.2 and 4.3 provide descriptions of key issues as well as existing initiatives to address these issues. Section 4.4 summarises input provided by participants on how they see the future of Indigenous data governance.

4.1 SURVEY

4.1.1 Engagement

A total of 6,687 users were reached through social media platforms promoting the survey. Of these users, there were 224 engagements (including likes, comments, shares, and clicks) with the posts. These engagements included 123 clicks on the link to the online survey. Social media posts were shared a total of 22 times by users on Facebook, Twitter, and LinkedIn. Table 2 summarises the total number of users reached on each platform and summarises the number of engagements with the post.

Table 2: Summary of engagement with social media posts

Platform	Language	Number of Users Reached	Number of Engagements (Likes, Comments, Shares and Clicks)	Number of Clicks
Facebook	English, French, and mixed English/French	582	20	11
Twitter	English and French	4,086	83	61
LinkedIn	English, French, and mixed English/French	1,369	92	51
Instagram	English, French, and mixed English/French	Not available	25	Not available
Indigenous Mapping Collective	English	Over 650	4	Not Available
Total:		**6,687**	**224**	**123**

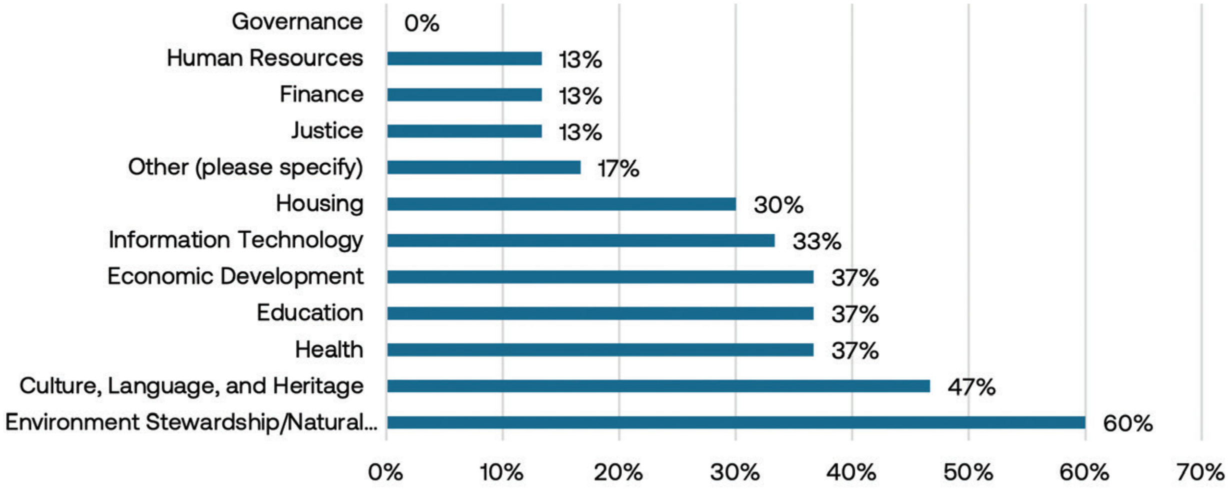
4.1.2 Participation

The online survey was launched on January 12th, 2021 and was closed on February 2nd, 2021. Thirty-seven people responded to the English language survey, of which 36 people consented to participate and one person declined to give their consent to participate. There were no completions of the French language survey.

Recognizing that data governance issues differ between Indigenous populations, and wanting to ensure that the research captured a broad range of perspectives on Indigenous data governance, participants were asked to identify which Indigenous population(s) they work/have worked with. Of a total of 30 respondents who completed this question, 29 reported working with First Nations data. Six respondents reported working with Inuit data and a further six reported working with Métis data.

Respondents noted working with a range of different data types (see Figure 1 below) including human resources; information technology; culture, language, and heritage; and natural resource management. Environmental stewardship data as well as culture, language, and heritage data were the most common data types that respondents reported working with.

Figure 1: Chart summarising the types of Indigenous data that survey participants work with in their roles.

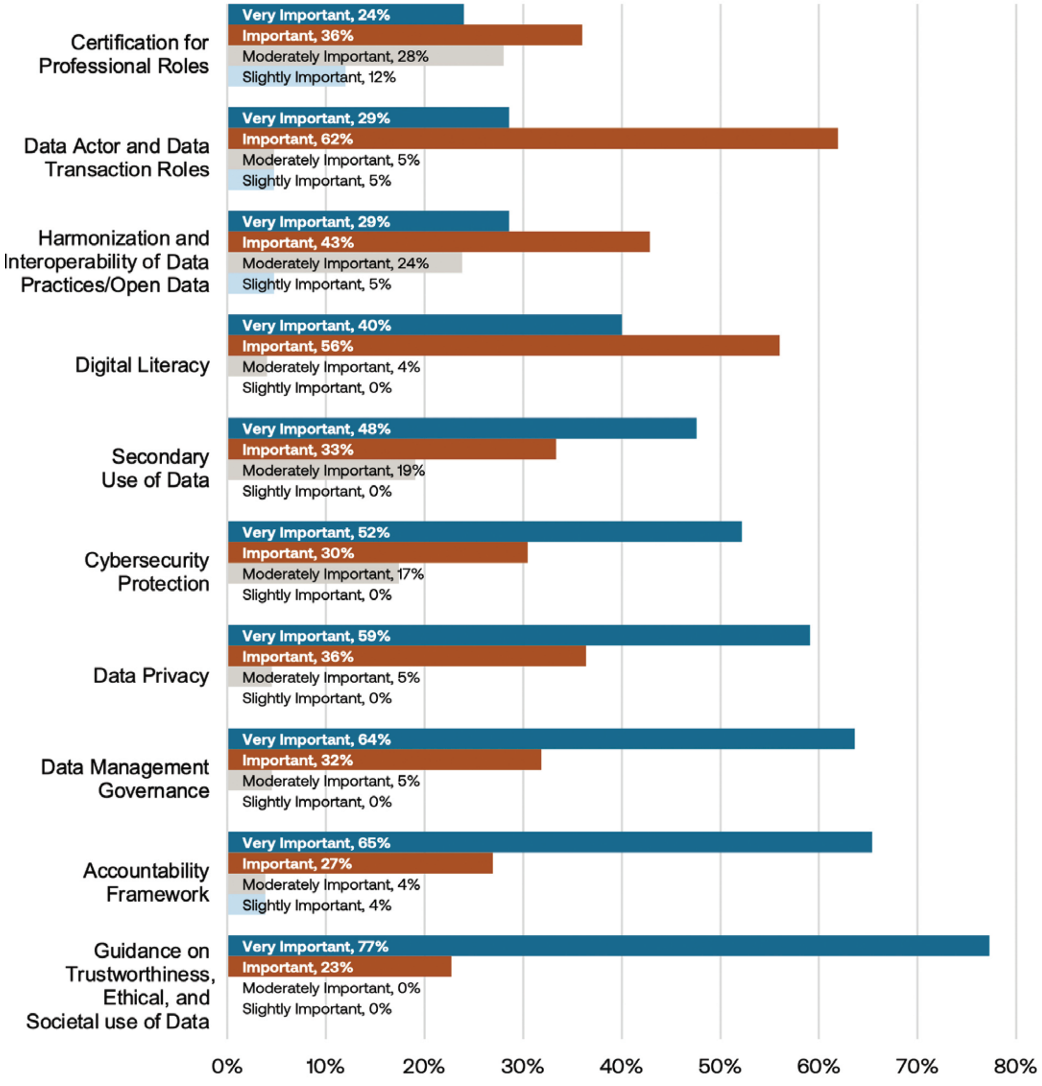


4.1.3 Ranking of Issues

Participants were presented with the ten key issues brought forward by DGSC Working Group 1 and were asked to rank each issue in terms of its importance for Indigenous data governance. Ranking was done on a five-point scale that ranged from *not important* to *very important* (*important* was the central measure). Participants were not asked to compare the issues with one another — the ranking was done individually for each of the 10 issues. An open-ended question was included after each ranking question in order to allow participants to further elaborate on their perspectives on each issue. The results of this ranking exercise are displayed in Figure 2 below.

Guidance on trustworthiness, ethical and societal use of data, and accountability frameworks were most frequently ranked by participants as being very important issues to focus on when developing data governance standards. Sixty-two percent of Participants agreed that establishing data actor and data transaction roles is an important issue; this issue was most frequently ranked as being important followed by Digital Literacy with 56%. None of the issues were ranked as not important.

Figure 2: Results of the survey ranking exercise for ten Foundations of Data Governance issues identified by DGSC Working Group 1



4.1.4 Comments on Key Issues

A series of themes emerged in participants' open-ended responses on the 10 key issues. Primary amongst these themes is the need to rebuild trust in relationships with Indigenous groups. Participants noted that trust is an integral component of the data lifecycle and upholding standards, and is a pivotal component to advancing Indigenous data governance and sovereignty.

Another theme that emerged revolved around the need to have Indigenous people leading and administering data collection programs in their communities, within their administrative jurisdictions, and for themselves. One participant, for example, noted that data collection has to be driven by Indigenous people and communities, not by external parties and systems.

While providing context on the top ranked issue — *Guidance on Trustworthiness, Ethical, and Societal Use of Data* — one Participant noted that it is very important to develop Indigenous-led ethics boards and review committees to provide approval, oversight, and interpretation of Indigenous data governance standards. Other key themes that emerged from Participants' responses to the ten key data governance issues are summarised in Table 3 below.

Table 3: Comments from survey respondents on key issues identified by Working Group 1

Key Issue	Qualitative Responses
Accountability framework	The primary themes on this issue include defining Indigenous data governance concepts and roles, developing culturally appropriate approaches to Indigenous data governance, and utilizing previously established principles such as OCAP® when establishing Indigenous data governance standards. Participants noted the following: It is important to define and differentiate between responsibility and accountability. Additionally, standards should ensure that institutions and researchers are accountable to the Indigenous groups they work with. The Privacy of Information Act is a good resource to provide guidance on developing standards for this issue. Additionally, some Indigenous governments and organizations have developed data sharing agreements to manage traditional knowledge — these can also be used as references. Some data types (e.g., land surveying data) are governed by foreign systems. In these cases, it can be challenging for an individual Indigenous group/organisation to establish accountability. Standards should address this issue. Ensure that the First Nations Principles of OCAP® are actually being practised and that organisations are not just using it as a buzz word.
Certification for professional roles	The primary themes on this issue included capacity development (i.e., training) and Indigenous data sovereignty. Participants noted the following: Certification and training should include components to improve the cultural competency of professionals who work with Indigenous groups. Standards for this issue should include polices that speak to monitoring and oversight that ensure a certain level of professionalism and ongoing certification for professionals. People who are responsible for Indigenous data (e.g., board members) need formal training on privacy standards. Alternatively, someone in the organisation should receive training and act in this capacity. The systematic barriers that create undue challenges for Indigenous people to collect, oversee, and make data-driven decisions on matters pertaining to their data and wellbeing need to be abolished.

Digital literacy	The primary theme on this issue was capacity (i.e., training). Participants noted the following: Digital literacy amongst the Indigenous population needs to be improved. This does not only include the skills to manipulate computer programs, but also includes the skills and knowledge to understand what happens to data after it has been collected and how data are handled.
Cybersecurity protection	The primary themes on this issue were funding and capacity development (i.e., training). Participants noted the following: Cybersecurity systems can be expensive to maintain (i.e., keep current). However, the quality of cybersecurity systems should not be overlooked. Standards should ensure high-quality systems are in place and functional — not just present. Indigenous groups need training to implement and assess their own systems and monitor their systems' interactions with other systems.
Data management governance	Primary themes on this issue included capacity development (i.e., technology and training) and trust. Participants noted the following: Additional training is needed within Indigenous communities to ensure that Indigenous-led data management and governance initiatives uphold Indigenous data sovereignty, locally, regionally, and nationally. Historically, data collected about Indigenous groups have not always been used in ways that positively impact Indigenous groups. Indigenous groups need to be included in all aspects of the development of Indigenous data governance standards. This will help build trust and accountability to citizens and hopefully result in greater participation and better/more data being collected.
Data privacy issues	Primary themes on this issue included trust, capacity (i.e., technology and training), and developing culturally appropriate standards. The three themes are closely related and revolve around the idea that the development of Indigenous data privacy standards must be led by Indigenous governments and organizations. However, before this can happen Indigenous groups must understand the issues. Additionally, once standards have been developed, Indigenous privacy officers will be needed to monitor compliance. One Participant noted that First Nations Principles of OCAP® should be used to guide this process. Another participant noted that there needs to be greater awareness of how provincial and federal privacy laws impact Free Prior and Informed Consent at the community, regional, and national level.
Trustworthiness, ethical, and societal use of data	Key themes on this issue included trust, capacity, ethics, Indigenous data sovereignty, and oversight. Participants noted the following: The First Nations Principles of OCAP®, as defined by First Nations right holders, should provide guidance on the development of standards for this issue in the context of First Nations data. One participant noted that greater support is needed for regional First Nation ethics boards and review committees to assert their own data sovereignty over information to ensure the data is not used without their approval, oversight, and interpretation. One participant also noted that "we must address our past, present, and future", concurrently. There is still a lot of trauma in communities that needs to be addressed to build trust and healthy relationships between all the players in the Indigenous data lifecycle.
Harmonization and interoperability of data practices	Key themes on this issue included culturally appropriate standards and capacity. Participants noted the following: While it is important for Indigenous groups to share data, this data sharing should not be to the detriment of Indigenous people. With this is mind, it was noted that standards must be guided by regional processes that have been initiated and supported by Indigenous protocols and practices to ensure access to data, reporting, and interpretation is inclusive.

Data actor and data transaction roles	Key themes on this issue included capacity development (i.e., technology and training), clear definition of roles, and developing culturally appropriate standards. Participants noted the following: Staff at Indigenous organisations should receive training to ensure that they can fulfill their data management job duties — both internally and externally. Additionally, staff should have access to the resources that they need to undertake their roles. Roles should be clearly defined, documented, and agreed upon. This can reduce overlap and eliminate gaps. In addition to having the skills to do the job, Indigenous data actors should be guided by standards with strong Indigenous-oriented ethical underpinnings.
Secondary use of data	Key themes on this issue included consent, ethics, and fulfilling regional ethical considerations. Participants noted the following: Currently, the collection, manipulation, interpretation, and resale of Indigenous data seems to be a largely unregulated open market. This needs to be addressed. Data transactions should include a standard consent that ensures data value retention, protection of participants, and respect. The consent should include clear explanation of who will access the data, how they will access the data, how long they will have the data, among other things. Consent should be communicated in culturally appropriate ways to ensure that Indigenous participants know what they are agreeing to. Regional oversight bodies should be engaged and strongly involved in the development of consent standards.

Participants were asked if there were other issues related to Indigenous data governance that were not covered in the list of 10 issues. One primary issue that was highlighted was data governance that pertain to photographs, songs, social media posts, interviews, and other data that are shared online or through day-to-day interactions. On this issue, participants noted that standards are needed to ensure that metadata are transmitted with primary data sets to ensure that Indigenous ownership and data rights can be tracked and maintained. Participants also noted that standards are needed to facilitate a tiered approach to consent, privacy, and giving permission. This tiered approach is focused on ensuring that a different level of permission can be given to family members, regional organizations, government, industry, or other entities when data and knowledge are being shared.

4.2 KEY ISSUES

This section gives an overview of the key issues that were raised during interviews and in open-ended responses to survey questions. This section draws primarily from the qualitative data collected during key participant interviews, expanding on issues raised in survey responses above. Where relevant, direct quotes from interviews are provided to more clearly illustrate the input provided during engagements.

4.2.1 Recognition of Authority

I would say the main obstacle to First Nations' data governance is the continuing lack of recognition of First Nations as sovereign governments. (I01)

A number of participants noted that a lack of recognition of the authority of Indigenous governments as sovereign decision-makers over all aspects of the life cycle of data relating to their populations and territories is the most significant data governance issue faced by Indigenous groups. The additional issues raised within this section were described by participants as a direct consequence of this main key issue. One key participant noted that recognition of this role for First Nations is indicated in some government documents but has not resulted in Nations being able to actively express sovereignty in practice.

Some of it is technical. Yes, First Nations need technical capacity, education, and training, etcetera. Some of it is cultural. First Nations need the space to express their information and data governance needs in ways that are culturally and linguistically relevant to them. But underneath all that – many of these questions could be answered by respecting through the body of legislation what the Federal Government is already committed to respecting in terms of preambles, in terms of public statements, in terms of signing treaties, and entering into agreements – the position of First Nations governments as sovereign governments with capacity and legal standing to pursue control over their own resources which include data and information resources. So, it's the political and legal standing that's the biggest challenge that separates First Nations from those challenges facing Canadians, I think. (I01)

Articles 3 and 4 of the United Nations Declaration on the Rights of Indigenous Peoples speak to the right to self-determination, as well as the means to finance their functions and pursue development goals. A number of survey and interview participants referenced these rights as the central underpinning of Indigenous self-determination and data sovereignty. Participants described a number of systemic barriers that exist to achieving recognition of Indigenous sovereignty to make decisions over how data is collected, stored, and used to make decisions related to their well-being. One participant referred to legislative and legal barriers as a form of institutional racism that prevents the advancement of Indigenous data sovereignty. Another participant observed that Indigenous data sovereignty, as a relatively new concept, is not something that government entities are prepared for.

The last thing is Indigenous data sovereignty in my mind seems to be a novel concept and a lot of government entities are not set up to, to permit it or, or only just beginning to make – create, create mechanisms that allow it to, to happen. (I06)

One example of this lack of preparedness was highlighted by another participant, who described their experience of a lack of understanding in the Federal Government of who exactly should be engaged with in the establishment and maintenance of Nation-to-Nation relationships. This lack of identification of the relevant Indigenous governing body perpetuates a lack of recognition of Indigenous sovereignty.

This lack of recognition has led to Indigenous groups not being included at the table when decisions are being made on issues relating to data governance.

And so, you know, part of what I envisioned data governance and sovereignty of data is starting to address that imbalance. But, when we're not even at the table I see pretty significant concerns. (I04)

Beyond being a presence at the table when discussing key issues, participants emphasised the need for Indigenous roles as decision makers in these processes. One participant noted this in relation to the DGSC process – that rather than being engaged on the issue of data governance standards, Indigenous groups should be part of leading the process of standards creation, in recognition of Indigenous self-governing authority.

I could start with just like a broader commentary on data governance in general and kind of make the parallels to the climate space, which is to say the majority of governance at both of those respective tables is done without the benefit of having First Nations to sit at the leadership table … but it's ironic to me that, you know, that there's not First Nations participation driving this whole [DGSC] process itself. And I think it's representative of the issues that First Nations face in trying to navigate through processes that are not respectful to their governance, their knowledge systems, their rights, you know. (I04)

Despite legislative barriers to assertion of authority over data, Indigenous groups continue to look for ways of exercising authority over data.

So, we're kind of in this space right now where we're – we want to assert and exercise our authority over our data, but the current legislative framework is creating these barriers. You know, that's one piece, but then the other piece is, you know, looking at this with our eyes wide open, do we need legislation to create that level of authority? Are there other ways that we can take and exercise authority and jurisdiction without using legislation? (I02)

Some participants described a level of recognition emerging in specific instances where provincial and federal bodies have entered into agreements that see data collection and management responsibilities being shared with Indigenous governments and organisations. A number of examples are listed in Section 4.3 below.

4.2.1.1 Capacity

The capacity of Indigenous governments and organisations to govern the collection, management, storage, and sharing of data was also raised as an issue by interview and survey participants. Capacity was described in terms of infrastructure, equipment, human resources, training, technology, and funding.

A number of issues were raised in relation to Indigenous organisations and governments not having the required equipment and technology to fulfill information governance functions. Participants described Indigenous governments utilising a wide range of technologies, from dealing exclusively with paper-based records to more modern information technology infrastructure. This range of approaches was described both within and between governments and can lead to loss and/or compartmentalisation of data.

The speed with which technologies become obsolete has left a number of organisations with data in unusable or inaccessible formats. This was noted in particular by participants in northern regions.

The first is generally just poor data practices and data infrastructure in my jurisdiction. We have big limitations in the Northwest Territories as a whole. Steps are being taken to, to improve that, but we're still far behind say compare to our – to say the best jurisdictions like B.C. or Ontario in my, my opinion. (I06)

One participant noted that while they are conducting Indigenous-led research with an Inuit organisation, capacity and infrastructure to store and manage data is not sufficient to keep up with requirements. Participants working in northern regions including the NWT and Yukon also noted challenges with staffing capacity, where high turnover and decreased availability of education and training opportunities hamper capacity to manage and govern data effectively.

One participant highlighted that among First Nations in their northern region, there is a lack of training in how data should be used and managed. Survey respondents also highlighted the need for increased training to increase digital literacy in Indigenous communities.

Survey respondents and key participants flagged that the training, staff, infrastructure, and equipment necessary to govern and manage data are expensive, and many Indigenous communities lack the long-term funding required to set up and maintain these systems. One participant noted that building capacity for increased data management capabilities within Indigenous governments can be deprioritised due to competing, pressing, immediate issues including improving standards of living. Two participants described how securing long-term funding was key for enabling their organisations to bolster capacity to the point that data strategies and policies could be developed to govern the collection, management, and use of data.

I mean as an organization I think we've for many years lacked the capacity to really develop and comprehensive data strategy. … To develop a data strategy so we could work towards, you know, data sovereignty and data governance, as well as – yeah, creating an engagement protocol with them. (Samantha Michaels)

Numerous survey and interview participants emphasised the need for reliable, long-term funding to invest in the capacity of Indigenous communities to achieve data sovereignty.

But if anything could stand out in that, in that report, I would recommend that it would be, you know, investing in First Nations capacity for data sovereignty is really the best way forward in, in them achieving and us achieving self-government. (I07)

And, the final thing that I'll just say … part of the kind of journey is how are we kind of investing in community-led capacity to do these things at, at the appropriate level. And often, you know, part of it is making sure that our communities have the ability to do this themselves without relying on others. (I04)

4.2.1.2 Access to Data

Participants in interviews and the survey emphasised that Indigenous governments and organisations do not have access to information about the populations they serve. With information housed by researchers, government and other organisations, Indigenous decision-makers lack the necessary information to govern. One participant expressed frustration at this lack of access to data.

And I, and I think that for many reasons because I don't understand how the Indigenous person, the Indigenous government, the Indigenous collective is not as valued as a non-Indigenous person's rights. Others have access to information much quickly. There's a process even, the ATIP [Access to Information and Privacy] process. There's all kinds of accountabilities that go back to citizens, but because that same opportunity's not provided us as Indigenous People, you wonder, are we valued as citizens? (I07)

In the Quebec context, participants noted that unique provincial legislation there can restrict access to data. Another participant gave an example of a research project on vulnerable Indigenous populations and law enforcement they were leading with an Indigenous organisation, where access to and ownership over data had to be negotiated with federal and other law enforcement bodies.

In some cases, access to data is only provided once certain conditions are met. One participant described an experience where access to necessary data was only afforded once capacity of the Indigenous organisation was built up to a sufficient level that it was recognised by federal and territorial government authorities – a process that takes considerable time and funding to achieve.

The second thing I think is difficult is you require a lot of capacity and a lot of investment by your organization when you want to get access to this Indigenous data. Especially when you get into the stuff that's more sensitive like health data. You need to demonstrate through governments that you have the capacity to manage this data. You have the continuity, you have the infrastructure, you have the policies. Like all of this has to be in place and this cost a lot of money and takes a lot of time. This stuff's – stuff is complicated. And it's got a lot of stipulations. And so, that's, that's a big barrier. (I06)

At the same time that participants raised concern with Indigenous groups not being able to access their data, survey respondents expressed frustration with Indigenous data being shared and sold by other secondary data users without appropriate oversight.

4.2.1.3 Culturally Appropriate Data

As outlined in Section 2.2, a large proportion of data collection and research conducted in Canada has not reflected the needs and priorities of Indigenous communities and data has been extracted from these communities on an ongoing basis. Participants in engagements also highlighted that data collection needs to be led by Indigenous organisations and data collection and management methods need to be reflective of the unique Indigenous cultural context, values, and norms relevant to each undertaking.

In discussing this issue, one interviewee noted that ethics boards governing research are more about managing risk than ensuring work is conducted in a manner appropriate for a certain community. Another participant gave an example of medical research conducted on First Nations in Nova Scotia that contravened the values of the community, but the ethics review process for the research had not engaged the community in decision-making and so was conducted without Indigenous oversight. A history of extractive research in Inuit Nunangat was highlighted by another interviewee.

… the four regions in Inuit Nunangat, and I mean before, you know, researchers could just come in willy-nilly and, and in some ways exploit the population or put people at harm or, you know, do research that was sure, important to, [a] university of this or that or whatever, but did it have any importance to the population or serve them in any way? (Samantha Michaels)

This history has led to heightened concerns among Indigenous populations regarding what information about individuals is being collected and shared. In one participant's experience, this can create challenges in building trust even with Indigenous-led data collection exercises. A survey respondent noted the need for trust-building to occur in order to assure Indigenous-led data collection has the support of communities.

The need for acceptance and inclusion of Indigenous science and ways of knowing and being as more appropriate means and method for collection of information about Indigenous groups was raised by a number of survey and interview participants. Participants expressed frustration at the dismissal and lack of respect for Indigenous knowledge systems and continued use of western science metrics that are not appropriate for use in an Indigenous context.

So there's – these key issues are not just about data sovereignty in the aspect of protecting information, it's also about sovereignty and having the autonomy to have your, your science and your ways of knowing and being accepted. Not validated, but accepted and equal to the scientific standards and western, western ways of doing data analysis. (I07)

And so, I guess, I guess that kind of is like a microcosm of the broader kind of data governance challenges of how are you, A: making sure that it's controlled and directed by First Nations based on, you know, the kind of combination of the different knowledge systems and worlds that they walk into. But then, B: how do you ensure that processes leading to outcomes are actually driven by those similar First Nations? And if not, then you, you risk essentially perpetuating that model of a disrespect towards First Nations knowledge and science and innovations. (I04)

The importance of not disconnecting data from its cultural context and removing it from Indigenous protocols and processes related to that data was emphasised by interviewees.

… once you disconnect that data from place there's an ability to manipulate it however you want and I think that's pretty problematic when considering kind of Indigenous data principles. Like, how are we, you know, remaining an accountable to community and place? And like what kind of protocols and processes that relate to that. Because once you remove it from that context, you also remove it from the system in which it's operating, you know. (I04)

One participant emphasised that alongside removing legislative barriers, space must be created for the creation and use of Indigenous-defined metrics and standards in relation to data. The potential for these metrics and standards to contribute to the enhancement of Indigenous well-being, through self-determination, was highlighted by a number of participants.

I think it's the breaking the barriers to achieving data sovereignty is the most important. And, and I think that means that the Federal Government, the people that make standards and create standards, provinces and other partners in Confederation, really need to make the investment in First Nations capacity to do this work. And the barriers are the legislation, and the standards themselves. They don't make space for First Nations to house information, you know, they don't create space for us to use our own metrics. (I07)

4.3 EXISTING STANDARDS AND INITIATIVES

A number of existing standards and initiatives were highlighted by participants that are of direct relevance to the potential development of Canadian data governance standards. These initiatives all assert the sovereignty of Indigenous Peoples to control all aspects of the collection, management, and use of their data. Indigenous-led standards and initiatives relating to data governance that emerged from engagements, as well as a brief review of relevant literature, are described below in Sections 4.3.1 to 4.3.3. A number of organisations and initiatives that were brought forward during engagements as relevant to the process of establishing data governance standards are briefly described in the list below.

- A number of initiatives have emerged in the field of Indigenous health where partnerships and data sharing agreements have been put in place with federal and provincial/territorial governments to enable Indigenous groups to lead the collection and management of Indigenous health data. Examples include the BC First Nations Health Authority; Northwest Territories Strategy for Patient-Oriented Research Unit: Hotıì ts'eeda; the First Nations Health And Social Secretariat Of Manitoba, Health Information Research Governance Committee; and the Information Governance and Data Projects (IGDP) office, which is housed at the Union of Nova Scotia Mi'kmaq (UNSM).
- The First Nations Information Governance Centre leads a number of initiatives and has produced a range of resources in relation to Indigenous data governance (including the examples provided below in Section 4.3.1 and 4.3.3).
- The First Nations of Quebec and Labrador Health and Social Services Commission has drafted a Quebec First Nations Information Governance Framework. The FNQLHSSC/CSSSPNQL is now working towards implementation of this framework.
- The BC First Nations Data Governance Initiative was established to run a number of demonstration projects to establish Indigenous data governance and sovereignty.

4.3.1 OCAP®

Contemporary Indigenous data sovereignty practices were led by First Nations in Canada. In 1998, the National Steering Committee (NSC) of the First Nations and Inuit Regional Longitudinal Health Survey (RHS) established a set of ethical data standards that ensure that the collection, dissemination, ownership, and use of data about First Nations is controlled and governed by First Nations. The First Nation Principles of Ownership, Control, Access, and Possession (OCAP®) establish the ethical collection, use, and storage of First Nations data, in keeping with each First Nation's respective worldview. The First Nations Information Governance Centre (FNIGC) holds the trademark on OCAP® for the benefit of all First Nations. The OCAP® principles were framed to reflect First Nations' values, protocols, and jurisdiction regarding data sovereignty. Although many Inuit and Métis organisations and governments have implemented protocols and principles similar to OCAP®, the OCAP® Principles do not constitute a Pan-Indigenous standard on data sovereignty.

Key participants emphasised that the OCAP® principles are an expression of First Nations sovereignty that speak to a Nation-to-Nation relationship with the Federal Government.

The OCAP® principles are something that others … including the Federal Government, need to understand and respect their role in making space for First Nations to exercise information governance as they see fit in pursuit of data sovereignty according to their own worldview … but it's really, really hard to get [non-First Nations] people to understand that their role in, quote, implementing OCAP®… has to be through that lens of sovereignty. That this is not just, you know, strong ethics or clear communications and acting with good intentions. There's a strong component around the exercise of sovereignty involving, you know, considerations over laws around intellectual property, considering lanes around jurisdictions, considering the entire, you know, constitutional historical relationship between First Nations and, and the Federal Government. (I01)

…how do we shift that narrative away from, you know, federal-led processes, provincial-led processes, where, you know, First Nations are asked to comment, and shift it towards, you know, this is kind of First Nations as self-directed and led work. And, you know, OCAP® is just kind of, I think a, I don't know, like a manifestation of that kind of giving power back to First Nations to drive, you know, their specific interests and priorities. (I04)

Participants in the survey and interviews described instances where OCAP® has been ignored due to lack of recognition of First Nations' authority, misinterpreted, or dismissed by organisations working with First Nations data. Despite these challenges, participants highlighted the continued importance and relevance of OCAP® as an expression of First Nations data sovereignty.

We own the inventions that come from our intellectual property. You may not access information in our community without coming through this process. It was circumvented. And consistently circumvented. People looked at that as like, "Well, that only comes from a resolution in an Indigenous organization that has the authority to, to – there's a governance structure around giving that resolution teeth, but it's not legal. We can break the OCAP® rules and, you know, beg for forgiveness instead of ask for permission". (I07)

In that OCAP® isn't scripture that's set in stone in 1998, these principles are living organic things. So, just as conceptions and practices of possessing data have changed in 2021, OCAP® can still be relevant and move along with that. (I01)

So, this is First Nations governance through the digital realm, right. And what does that look like? Well, we're still figuring that out. But that, that is the challenge of OCAP®, I think, today. This idea of possession – the retention of ownership rights and the possession and all of the things that that implies over something ephemeral like data. And that was probably the case in the '90s, but it's even more so the case now. (I01)

4.3.2 First Nations National Data Governance Strategy

In March 2020, the First Nations Information Governance Centre submitted a report to Indigenous Services Canada entitled, A *First Nations Data Governance Strategy* (FNDGS) that offered a realistic path to achieving First Nations data sovereignty. It sets out two short-term strategic priorities: 1) establishing Data Champion Teams in each region and at the national level; and 2) securing bridge funding for pre-implementation activities. Next, FNIGC and its partners will develop a national business case to access Budget 2021 funding should it be made available.

The FNDGS is grounded in “community-driven and Nation-based” principles. It presents nine pillars for action that outline where First Nations data capacities need to be built. It includes a phased implementation plan, a maturity model, and an accountability framework. It is important to note that the Strategy is a complex and multifaceted systems transformation initiative and it covers new uncharted territory with very few baselines and experiences to draw from. Its ambitious goal is to establish a network of ten semi-autonomous regional and one national First-Nations-led information governance centres across Canada, as envisioned by First Nation rights holders. The Strategy makes a strong case for such a network and tangibly demonstrates how it will impact outcomes in the short, medium, and long terms.

A number of participants emphasised the importance of the FNDGS as a guiding document on the steps necessary for Nations to achieve data sovereignty.

So, basically, the future scenario is 11 First Nations-led statistical institutes across Canada: 10 regional and one national. Where First Nations rights holders (communities, Nations, and their leaders) have full control over their data through the governance of their regional information or statistical centre. Each Centres’ governance structure should reflect the Nations in that region. (I02)

These Centres will also be equipped with the expertise, capacities, and the infrastructures needed, and that are on par or in line with other statistical institutions in Canada, such as Statistics Canada. Building First Nations institutions however does not mean tearing down existing ones. (I02)

Each regional data governance centre to be established as part of the FNDGS would be rooted in First Nations’ values, languages, and conceptions of collective ownership.

As we move toward implementation, we need to consider options for how collective ownership and control of our data can be achieved. There is nothing within the current legislative framework that supports this. The Privacy Act for example, protects individual privacies; it would have to be revamped to accommodate for collective protections. (I02)

The importance of continued, long-term funding to build the capacity necessary to advance the FNDGS was also emphasised as a necessary step to achieving success.

So, political will is one thing, having the actual capacity to move it forward is another. So, in this data strategy, it’s actually about an incremental ten-year move forward, building governance and human resource capacity as we do all of this other work. (Gwen Phillips)

4.3.3 National Inuit Strategy on Research

In 2018, the National Inuit Strategy on Research (NISR) was established to reform the harmful research practices conducted by external actors on Inuit Nunangat communities. NISR establishes a set of research principles that assert Inuit governance over how data and information on Inuit, wildlife, and the environment is collected, stored, used, and shared. NISR emphasizes that external researchers must engage with Inuit in a way that recognizes the self-governing and self-determining authority of Inuit. NISR also asserts that all research conducted on Inuit, wildlife, and environment must be carried out with the purpose of benefiting Inuit. NISR is organized into two sections:

1. An outline of the Inuit vision for research and the notion that Inuit research is strongly associated with the broader goal of achieving social and economic equity for Inuit, and
2. Five priority action areas towards attaining Inuit governance over research data and information collected in Inuit Nunangat.

Priority action item number four is of particular relevance, as the goal of this action area is to "ensure Inuit access, ownership, and control over data and information". The accompanying NISR Implementation Plan outlines deliverables along with key decision-makers and partners involved in achieving milestones towards this goal within the 5-year timeframe of the NISR. A number of committees at ITK, including the Inuit Qaujisarvingat National Committee (IQNC) and National Inuit Data Management Committee, are a key part of implementation of this plan.

4.4 THE FUTURE OF INDIGENOUS DATA GOVERNANCE

While initiatives such as the FNDGS and NISR track a clear path forward for First Nations and Inuit data governance and sovereignty, respectively, participants shared a number of general elements of what the future of Indigenous data governance and data governance standards should look like.

Broadly, participants emphasised that data sovereignty is a necessary part of and precursor to a broader move towards achieving self-determination.

I don't separate, you know, the aspirations of data governance and sovereignty from the broader kind of project of, you know, First Nations self-determination. Because I think like the plight and the objective of, you know, upholding Indigenous data sovereignty is also in-line with upholding Indigenous self-determination, First Nations self-determination in particular. (I04)

Nation-to-Nation relationships through data sharing agreements were brought forward as important means of advancing Indigenous data sovereignty and self-determination. Standards relating to Indigenous data governance should be based on and linked to these relationships.

But that is paramount to the standardization thing, is to think about the actual relationship that the standards attach to. So, they can't do it as a pan-exercise. (Gwen Phillips)

In order to develop and maintain these relationships, participants underlined the need for federal and provincial/territorial governments to build their capacity to understand and engage with Indigenous Peoples. Examples provided included building cultural competency and understanding of the history of Indigenous data governance.

And the last thing that I want – it's weird. It's like the catch-22, it's like, you know, these federal governments need to build more capacity to understand Indigenous Peoples and engage with them. And I would say this is a similar context for data governance, they need to understand what, you know, Indigenous data governance and sovereignty means, and you know, the history and what not. (I04)

Building and maintaining relationships between self-governing Indigenous governing bodies on the establishment of data management systems was also highlighted as an important path forward in order to ensure inter-operability and avoiding duplication of efforts.

There is opportunity to collaborate and build a data management system that can meet everyone's needs and increase interoperability, sharing among FNs so that we aren't always reinventing the wheel, and facilitate improved ability to participate in co-management and implementation of final agreements. I11

Data governance laws, standards, and quality indicators that are reflective of Indigenous values and knowledge systems, and defined and administered by empowered self-determining Indigenous governing bodies, are an important part of this future. One survey participant underlined these as crucial to collecting better data and building trust and accountability to citizens.

We know we have to have standards. And so, defining quality is one of the very, very important pieces. (Gwen Phillips)

We need to think strategically about empowering institutions to support Nation rebuilding. Again, that's what – having confidence in data and having a master data strategy with standards. (Gwen Phillips)

And when we're considering that within kind of an Indigenous way of knowing or First Nations way of knowing, you know, it's inclusive of our languages, it's inclusive of our stories, of our ceremonies, of our songs, of our pictographs, you know, depending on where you are. And so, you know, being clear on what data is within this context is I think really important. (I04)

Survey respondents highlighted that training will be needed for Indigenous leaders and data governance specialists in order to implement Indigenous-defined standards. Participants also highlighted that this should be coupled with training for all others involved in the data life cycle, including multiple levels of government from federal to municipal, on the different roles and responsibilities of each party. The potential need for establishment of professional standards for those working in Indigenous data management was also highlighted by one participant, along with the need for Indigenous privacy officers to monitor standards compliance.

5. Recommendations

5.1 RECOMMENDATIONS

Based on the input provided during engagements, a number of recommendations are provided below relating to the continued engagement and involvement of Indigenous governments and organizations in the DGSC process.

1. Additional engagement of Inuit and Métis organisations and data governance experts is required. Due to limited participation of Inuit and Métis practitioners and experts in engagements, further work is required in order to capture the perspectives of these key Indigenous groups on data governance issues and on the work of the DGSC.
2. Further involvement of Indigenous governments and organizations in the DGSC process will be necessary in order to dedicate the time and resources necessary to clearly defining issues brought forward by Indigenous governments and organizations and integrating them, where appropriate, into issues already defined by DGSC working groups. This may also include participation of Indigenous representatives on DGSC working groups. For example, based on their high ranking in survey results, a number of key issues from Working Group 1, including *Guidance on Trustworthiness, Ethical, and Societal use of Data*, Accountability Framework, and Data Management Governance will require further input from Indigenous peoples.
3. Identifying key Indigenous organisations (including those already developing standards or principles such as Inuit Tapiriit Kanatami and the First Nations Information Governance Centre, respectively) to participate in further phases of DGSC work, including standards development, will be a necessary outcome of further engagements.

5.2 CLOSURE

Should you wish to discuss any aspect of this report further, please do not hesitate to contact Guy Polden at the Firelight Group.

T: +1 (778) 851-0264
E: guy@firelight.ca

Citations

Espey, J. *Stewardship and OCAP®*. First Nations Statistical Institute. 2002.

First Nations Information Governance Centre. “Ownership, Control, Access and Possession (OCAP®): The Path to First Nations Information Governance.” 2014.

First Nations Information Governance Centre. “Pathways to First Nations’ Data and Information Sovereignty.” In *Indigenous Data Sovereignty: Towards an Agenda*, edited by Tahu Kakutai and John Taylor, 139-155. The Australian National University: ANU Press, 2016.

First Nations Information Governance Centre. “First Nations Data Sovereignty in Canada.” *Statistical Journal of the IAOS*. (s2019): 1–23. https://doi.org/10.3233/SJI-180478.

Inuit Tapiriit Kanatami (ITK). *National Inuit Strategy on Research*. 2018.

Kukutai, Tahu, and John Taylor. Indigenous Data Sovereignty: Toward an Agenda. Acton, Australia: ANU Press, 2016.

Lovett, Raymond, Vanessa Lee, Tahu Kukutai, Donna Cormack, Stephanie Rainie, Jennifer Walker. “Good data practices for indigenous data sovereignty and governance.” In *Good Data*, edited by Angela Daly, S. Kate Devitt, Monique Mann, 26-36. Institute of Network Cultures, 2019.

McBride, Kate. *Data Resources and Challenges for Nations Communities*. Alberta First Nations Information Governance Centre (AFNIGC). 2018.

McMahon, Rob, Trevor James Smith, and Tim Whiteduck. “Reclaiming Geospatial Data and GIS Design for Indigenous-led Telecommunications Policy Advocacy: A Process Discussion of Mapping Broadband Availability in Remote and Northern Regions of Canada.” *Journal of Information Policy* 7 (2017): 423-449.

Raine C. Stephanie, Jennifer. L. Schultz, Elleen Briggs, Patricia Briggs, Nancy Lynn Palmanteer-Holder. “Data as a Strategic Resource: Self-Determination, Governance, and the Data Challenge for Indigenous Nations in the United States.” *The International Indigenous Policy* Journal 8, 2, (2017). 1-29.

Raine C. Stephanie, Tahu Kukutai, Maggie Walter, Oscar Luis Figueroa-Rodríguez, Jennifer Walker, and Per Axelsson. “Indigenous data sovereignty.” In *The State of Open Data*, edited by Tim Davies, Stephen B. Walker, Mor Rubinstein, Fernando Perini, 300-319. African Minds, IRDC, 2019.

Royal Commission on Aboriginal Peoples (RCAP). The *Report of the Royal Commission on Aboriginal Peoples*. 1996.

Smith, E. Diane. “Governing data and data for governance: the everyday practice of Indigenous sovereignty.” In *Indigenous Data Sovereignty: Towards an Agenda*, edited by Tahu Kakutai and John Taylor, 117-135. The Australian National University: ANU Press, 2016.

Snipp, C. Matthew. “What Does Data Sovereignty Imply: What Does It Look Like?” In Indigenous Data Sovereignty: Toward an Agenda, edited by KUKUTAI TAHU and TAYLOR JOHN, 39-56. Acton ACT, Australia: ANU Press, 2016. Accessed February 25, 2021.

Steffler, Jeanette. “The Indigenous Data Landscape in Canada: An Overview.” *Aboriginal Policy Studies*, 5, 2, (2016): 145-164.

Truth and Reconciliation Commission of Canada (TRC). *The Final Report of the Truth and Reconciliation Commission of Canada*. 2015.

Appendix 1: Interview Consent Form

INDIGENOUS ENGAGEMENT ON THE CANADIAN DATA GOVERNANCE STANDARDIZATION COLLABORATIVE – KEY INFORMANT INTERVIEW

Declaration of Informed Consent and Permission to Use Information

I (name) ______________________________________ , on this day (complete date) ________________ , give permission for Firelight Research Inc. to interview me for the Indigenous engagement on the Canadian Data Governance Standardization Collaborative.

I understand that this interview is being conducted by Firelight Research Inc. The purpose of the study is to get initial input from Indigenous groups on the unique data governance issues faced by Inuit, Métis and First Nations, describing Indigenous perspectives on how these issues could be addressed and describing existing initiatives relating to Indigenous data governance and sovereignty.

By signing below, I indicate my understanding that:

1. I consent to have my words and responses recorded in notes and on the zoom recording;
2. I am free to not respond to questions that may be asked and I am free to end the interview at any time I wish.
3. Individual participants in this research will remain the owners of their respective responses provided during key informant interviews. Each interview participant will be provided with their interview recording and transcript following the interview. Participants will retain rights to the interview audio and transcript. Participants will be provided a copy of the report produced as a result of this study. Participants will review the report and hold the right to make any changes to interpretations or quotes prior to publishing. Interview data will be stored on a secure Canada-based server owned and operated by Firelight. All data will be deleted from the server within one year of being collected.

For more information, please contact Guy Polden (604) 345-7532

I would like my quotes included in the report. I understand that I hold the rights to withdraw my consent:

yes **no**

I would like my name included in the report. I understand that I hold the rights to withdraw my consent:

yes **no**

Signature of participant ______________________________________

Witness ______________________________________

PIN #:

Appendix 2: Survey

This survey is being administered by The Firelight Group on behalf of the Canadian Data Governance Standardization Collaborative (DGSC). Firelight is reaching out to Indigenous representatives, knowledge holders, and data governance experts to gather information about Data Governance from an Indigenous perspective. The information will be used to support the development of the Canadian Data Governance Standardization Roadmap.

What is the Data Governance Standardization Collaborative?

The DGSC was established in 2019 to coordinate Data Governance standardization strategies across Canada. The DGSC is not tasked with the developing the actual standards. Its role is to: enable stakeholders to focus their resources, articulate stakeholders' needs, propose coordinated standardization activity, and minimize duplication of effort — on matters pertaining to Data Governance in Canada.

Data Governance strategies refer to best practices that guide the collection, usage, storage, archiving, transfer, disposal, and purging of Data. The DGSC's roadmap will describe the current and desired state of Data Governance in Canada. The roadmap will also identify gaps, make recommendations to fill the gaps, establish priorities for action, and suggest organizations that will eventually develop the Data Governance standards.

What is this survey about?

This is Phase 1 of a 2-Phase process. In this phase, Firelight is reaching out to Indigenous representatives and knowledge holders, and Data Governance experts to get their perspectives on how Indigenous perspectives can be incorporated in the Data Governance strategies. The information that you and other participants share in this survey will be used to develop a report on Indigenous Data Governance that will be submitted to the DGSC. Phase 2 will commence in summer 2020 and will build on the work done in Phase 1.

Consent Page

Your participation in this survey is completely voluntary. You may refuse to take part in the research or exit the survey at any time without penalty. You are free to decline to answer any particular question you do not wish to answer for any reason. The information you will share with us will be kept completely confidential.

This survey is being administered by The Firelight Group. The Firelight Group is an indigenous owned company with over 10 years of experience carrying out carrying out community-based research in Indigenous communities across Canada. To find out more about Firelight, please visit our website at https://firelight.ca.

Contact Information

If you need more information about this project, please contact:
Guy Polden (guy.polden@firelight.ca)

So far, the DGSC has explored 35 key issues related to Data Governance. We are seeking your input on the Indigenous perspective on 10 of the key issues; the others will be explored in Phase 2. The questions will focus on:

1. Current research – people or organizations carrying out research on each issue;
2. Priorities – which Data Governance issues are of the highest priority;
3. Gaps – where work is need to develop Indigenous Data Governance standards; and
4. Recommendations – how can Data Governance be improved? What needs to be done?
5. Research and Development – people or organisation who should carry out research and development of Indigenous focused Data Governance standards.

PART 1

1. Data Governance issues differ between Indigenous populations and we want to make sure we capture a broad range of perspectives on Indigenous Data Governance. Please select the Indigenous population(s) below whose data you work/have worked with:

   □ First Nations

   □ Inuit

   □ Métis

   □ Other Indigenous Group(s) (please specify).

2. Which Indigenous sector(s) do you work with?

   □ Health

   □ Justice

   □ Governance

   □ Natural Resource Management

   □ Information Technology

   □ Finance

   □ Other (please specify)

PART 2

In the next set of questions, we will ask you to rate the level of importance of 10 Data Governance issues. We want to know the importance of these issues from an Indigenous perspective.

For each issue, we will provide a definition and then ask you to rate its importance on a scale of 1-5 where 1 is not important and 5 is very important.

Accountability Framework

This issue covers the liability and the control structure for all data collected and created, and clarifies the roles, responsibility and accountability of data transaction. The responsibility of the data rights holder, the implication of ownership transfers, and the notion of consent will also be explored.

3. On a scale of 1-5 please rank the importance of addressing Accountability Framework issues when developing Indigenous Data Governance standards.

   □ Very Important

   □ Important

   □ Moderately

   □ Slightly Important

   □ Not Important

Certification for Professional Roles

This issue clarifies the role of professionals working with data and information, explore certifications programs that should be developed, and the requirement of the industry. This issue should first be addressed by assessing professional competencies requirement based on a clear framework representing the backbone of data governance.

4. On a scale of 1-5 please rank the importance of addressing Certification for Professional Roles issues when developing Indigenous Data Governance standards.

Digital Literacy

It was determined this issue will cover digital literacy by focusing on improving the understanding of data, technology, and interfaces of Canadian residents. Digital literacy must be kept separate than professional certification and have a broader mandate including the use of technologies effectively and securely. Education represents a key mechanism to raise Canadians' awareness on the challenges and opportunities of an increasingly digital society, which is necessary for the implementation of efficient and inclusive data governance framework.

5. On a scale of 1-5 please rank the importance of addressing Digital Literacy issues when developing Indigenous Data Governance standards.

   □ Very Important

   □ Important

   □ Moderately

   □ Slightly Important

   □ Not Important

Cybersecurity Protection

This issue covers Cybersecurity protection and transparency, which are transversal components across the data governance framework. Cybersecurity threat will increase with the rise of technology and will require stronger mechanisms to protect data and sensitive information. The core of cybersecurity risks is related to digital, network, and connectivity infrastructure.

6. On a scale of 1-5 please rank the importance of addressing Cybersecurity Protection issues when developing Indigenous Data Governance standards.

   □ Very Important

   □ Important

   □ Moderately

   □ Slightly Important

   □ Not Important

Data Management Governance

This issue explores the necessity of planning, oversight, monitoring, and compliance of data management at the organizational level, aiming to clarify how data should be managed throughout its lifecycle. Data management should include the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets. This issue should also consider a framework that will allow for the review of data management at the organizational level.

7. On a scale of 1-5 please rank the importance of addressing Data Management Governance issues when developing Indigenous Data Governance standards.

   □ Very Important

   □ Important

   □ Moderately

   □ Slightly Important

   □ Not Important

Data Privacy

This issue explores the necessity of planning, oversight, monitoring, and compliance of data management at the organizational level, aiming to clarify how data should be managed throughout its lifecycle. Data management should include the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets. This issue should also consider a framework that will allow for the review of data management at the organizational level.

8. On a scale of 1-5 please rank the importance of addressing Data Privacy issues when developing Indigenous Data Governance standards.

   □ Very Important

   □ Important

   □ Moderately

   □ Slightly Important

   □ Not Important

Guidance on Trustworthiness Ethical & Societal use of Data

The issue explores trustworthiness and ethical use of data in accordance to the Canadian privacy expectations specified in PIPEDA and the Privacy Act. This issue aims to clarify the ethical use of data with respect to who owns data or stewards, and the ethical and societal use of data according to public value. There should be a better understanding of what it takes from data owners, data stewards, the public, and providers to be trustworthy to collect, manage, hold and use data, and actively demonstrate this trustworthiness throughout the lifecycle.

9. On a scale of 1-5 please rank the importance of addressing Guidance on Trustworthiness Ethical & Societal use of Data issues when developing Indigenous Data Governance standards.

   □ Very Important

   □ Important

   □ Moderately

   □ Slightly Important

   □ Not Important

Harmonization & Interoperability of Data Practices/Open Data

This issue explores the necessity of planning, oversight, monitoring, and compliance of data management at the organizational level, aiming to clarify how data should be managed throughout its lifecycle. Data management should include the development, execution, and supervision of plans, policies, programs, and practices that control, protect, deliver, and enhance the value of data and information assets. This issue should also consider a framework that will allow for the review of data management at the organizational level.

10. On a scale of 1-5 please rank the importance of addressing Harmonization & Interoperability of Data Practices/Open Data issues when developing Indigenous Data Governance standards.

    □ Very Important

    □ Important

    □ Moderately

    □ Slightly Important

    □ Not Important

Data Actor and Data Transaction Roles

This issue covers the roles of data actors throughout the lifecycle of the supply chain. Between the data collection and data consumption, there is a huge layer of data management processes. There are numerous people involved through the lifecycle of even a single data element; whether it is securing the data from unauthorized access or taking daily backups for example. These different actors are then accountable for protecting data through the formation of a secure system that reduces any risks of errors. Thus, this issue highlights the responsibility of data professionals and the accountability of their role.

11. On a scale of 1-5 please rank the importance of addressing Data Actor and Data Transaction Roles issues when developing Indigenous Data Governance standards.

    □ Very Important

    □ Important

    □ Moderately

    □ Slightly Important

    □ Not Important

Secondary Use of Data

This issue covers the secondary use of data. Secondary use of data is defined as the use of data that is not that for which it was originally collected. Secondary use includes data for a different purpose than what the data rights holder had initially consented and for which explicit consent was not received.

12. On a scale of 1-5 please rank the importance of addressing Secondary Use of Data issues when developing Indigenous Data Governance standards.

    □ Very Important

    □ Important

    □ Moderately

    □ Slightly Important

    □ Not Important

PART 3

For the final set of questions, we will be asking about current work being done on Data Governance by Indigenous organisations.

13. Are there any other issues related to Indigenous Data Governance that is not captured in the list?

    □ Yes

    □ No

14. If yes, please state.

    ____

    ____

15. Are you aware of any ongoing research that is focused on developing Indigenous Data Governance standards?

    □ Yes

    □ No

16. If yes, who is carrying out this research?

    ____

    ____

17. What is the focus of the research?

    ____

    ____

18. Do you know about any existing Indigenous Data Governance standard(s) that could be applicable on a National Basis?

    □ Yes

    □ No

19. If yes, please us about it/them.

    ____

    ____

20. Do you know of any person or organisation that would be a good candidate to develop Data Governance standards from an Indigenous perspective?

    □ Yes

    □ No

21. If yes, please state.

    ____

    ____

Thanks for participating in the survey!

Appendix 3: Interview Guide

INDIGENOUS ENGAGEMENT ON THE CANADIAN DATA GOVERNANCE STANDARDIZATION COLLABORATIVE – KEY PARTICIPANT INTERVIEW GUIDE

This guide includes:

- Background to the study; and
- Interview questions.

Introduction

Firelight is reaching out to Indigenous organisations, representatives, and data governance experts to gather perspectives on Indigenous data governance and sovereignty. The information will be used to provide recommendations on the development of the Canadian Data Governance Standardization Roadmap. Our research aims to get initial input from Indigenous groups on the unique data governance issues faced by Inuit, Métis and First Nations, describing existing Indigenous standards relating to data governance (e.g., OCAP®) and Indigenous perspectives on how these issues could be addressed. The report produced as a result of this research will feed into DGSC's roadmap document. This report will have distinct sections pertaining to the unique issues and perspectives of Inuit, Métis and First Nations groups and will provide a series of recommendations based on the input and guidance gathered during the research.

Background

What is data governance?

Data governance is a broad concept, but essentially means the people, organisations and processes that are set up to make decisions about how information is collected, managed, stored, accessed and shared.

What is the Data Governance Standardization Collaborative?

The DGSC was established in 2019 to coordinate data governance standardization strategies across Canada. The DGSC is not tasked with developing the final standards. The role of the DGSC is to: enable stakeholders to focus their resources, articulate stakeholders' needs, propose coordinated standardization activity, and minimize duplication of effort — on matters pertaining to data governance in Canada.

Data governance standards refer to best practices that guide the collection, usage, storage, archiving, transfer and disposal of data. The DGSC's roadmap is being drafted by 4 cross-sector working groups and will describe the current and desired state of data governance in Canada. The roadmap will also identify gaps, make recommendations to fill the gaps, establish priorities for action, and suggest organizations that will eventually develop data governance standards.

A number of issues were identified by the working groups, but as Indigenous groups are not represented on the working groups, our research aims to seek initial input from Inuit, Métis and First Nations on data governance issues faced by Indigenous peoples.

The primary goals of this research are to discern:

- What are the main data governance issues or challenges that Canadian Indigenous groups currently face?
- What standards currently exist that relate to Indigenous data governance and sovereignty?
- What is the ideal future scenario for Indigenous data governance and sovereignty, according to First Nations, Métis and Inuit groups?
  - How is this achieved?
  - Who should be involved in the process?
- What role should data standards play in this future scenario?

How information collected will be used.

Informed consent will be obtained from each survey respondent and interview participant. The information that you and other participants share as part of this research will be used to develop a report on Indigenous data governance that will be submitted to the DGSC. This report will provide a series of recommendations based on the responses provided by participants, including how Indigenous groups could continue involvement in this process.

This preliminary research aims to identify issues of concern for Indigenous data governance. Further research is required to develop, or indeed decide if it is appropriate to develop, Indigenous data governance standards. Further research will be conducted based on recommendations provided as a result of this research and in a manner consistent with best practices as determined by Indigenous experts and leaders in the field.

*[Read the below with **recording on** at the start of each interview.]*

Today is [date]. We are interviewing [participant name] for Firelight's Indigenous Engagement on the Canadian Data Governance Standardization Collaborative. Thank you for coming. My name is [name] and my co-researcher(s) is/are [name]. We're conducting this interview today over zoom videoconferencing software. [Participant name] has read and signed the consent form, and we have assigned them participant ID [number]. We have explained the purpose of the study and the interview plan.

1. **Background Questions**
   - Can you briefly describe your work and how it involves governance of Indigenous data?
2. **Data Governance Issues**
   - What are the main data governance issues or challenges that Canadian Indigenous groups currently face?
   - What are the most important issues to focus on?
   - In your opinion, do you think the issues are different for Inuit, First Nations and Métis groups?
3. **Existing Standards and Initiatives**
   - What standards currently exist that relate to Indigenous data governance and sovereignty?
   - How successfully have these initiatives addressed Indigenous data governance issues?
   - What barriers exist to the success of these standards/initiatives?
   - What role do these existing standards/initiatives play in strengthening Indigenous data sovereignty/governance?

4. **Future**
   - What is the ideal future scenario for Indigenous data governance and sovereignty?
   - How do we get there?
   - Who should be involved in the process?
   - What role do you think data standards play in the future scenario that you envision?

Conclusion

Read with audio and video recorders on after every interview.

Today is [date]. We have just finished interviewing [participant name] for Firelight's Indigenous Engagement on the Canadian Data Governance Standardization Collaborative Research Project.

My name is [name] and my co-researcher(s) is/are [name]. We conducted this interview today over zoom. This interview has taken approximately [#] hours [#] minutes.

Appendix 4: Engagement Materials

SOCIAL MEDIA POSTS (TEXT)

Facebook/LinkedIn:

There is a long history of poor data collection and misuse of information collected about Indigenous populations in Canada. Currently, many First Nations, Inuit, Métis and other Indigenous groups and organisations are striving towards the concept of data sovereignty. Decisions on data governance standards cannot be made without the close involvement of Indigenous groups. The Firelight Group is working with the t to conduct a survey that asks: What are the main data governance issues or challenges that Indigenous groups currently face?

Visit https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey to complete the survey. Fill out the survey for the chance to win a $100 gift card to the business of your choice!

Questions? Contact Guy Polden at The Firelight Group.
Email: guy.polden@firelight.ca

French

Les collectes de données au sujet des peuples autochtones du Canada et l'utilisation des informations recueillies demeurent trop souvent déficientes et inadéquates. Plusieurs Premières Nations, ainsi que les Inuit, Métis et autres groupes autochtones visent à atteindre le concept de souveraineté des données. Les décisions concernant les normes de gouvernance des données ne peuvent être prises sans une collaboration étroite avec les groupes autochtones. Firelight Group travaille en collaboration avec le Conseil canadien des normes afin de mener un sondage et de poser la question suivante : Quels sont les principales problématiques de la gouvernance des données ?

Visiter le https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey pour répondre au sondage et courez la chance de remporter une carte-cadeau de 100$ au magasin de votre choix.

Contactez Guy Polden de chez Firelight pour plus de détails.
Email: guy.polden@firelight.ca

Twitter:

The Firelight Group is working with the Canadian Data Governance Standardization Collaborative to conduct a survey that asks: What are the main data governance issues or challenges that Indigenous groups currently face?

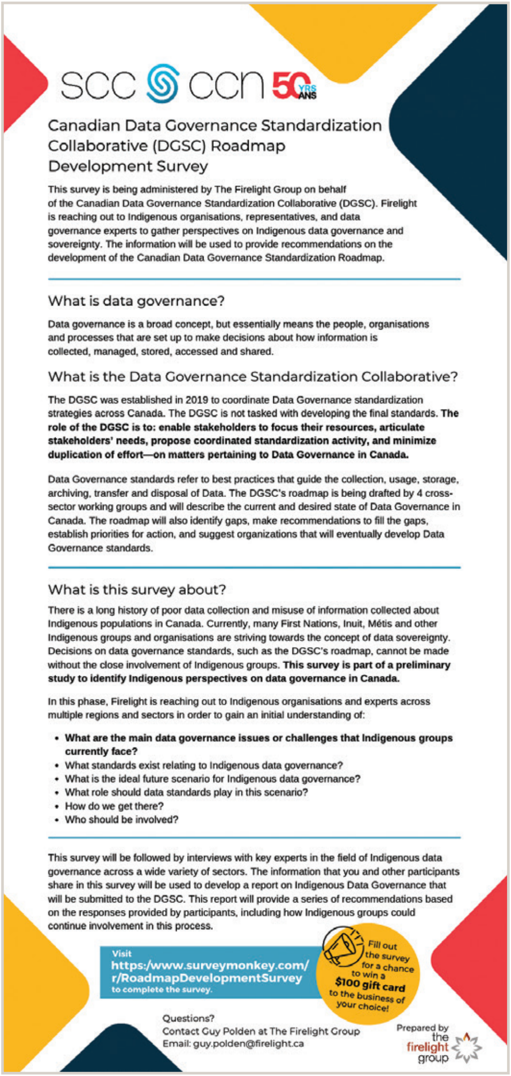
Visit https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey
to complete the survey. Fill out the survey for the chance to win a $100 gift card to the business of your choice!

French

Firelight Group travaille en collaboration avec le Conseil canadien des normes afin de mener un sondage et de poser la question suivante : Quels sont les principales problématiques de la gouvernance des données ?

Visiter le https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey pour répondre au sondage et courez la chance de remporter une carte-cadeau de 100$ au magasin de votre choix.

SOCIAL MEDIA POSTS (GRAPHICS)



SCC CCN 50 YRS ANS

Canadian Data Governance Standardization Collaborative (DGSC) Roadmap Development Survey

This survey is being administered by The Firelight Group on behalf of the Canadian Data Governance Standardization Collaborative (DGSC). Firelight is reaching out to Indigenous organisations, representatives, and data governance experts to gather perspectives on Indigenous data governance and sovereignty. The information will be used to provide recommendations on the development of the Canadian Data Governance Standardization Roadmap.

What is data governance?

Data governance is a broad concept, but essentially means the people, organisations and processes that are set up to make decisions about how information is collected, managed, stored, accessed and shared.

What is the Data Governance Standardization Collaborative?

The DGSC was established in 2019 to coordinate Data Governance standardization strategies across Canada. The DGSC is not tasked with developing the final standards. **The role of the DGSC is to: enable stakeholders to focus their resources, articulate stakeholders' needs, propose coordinated standardization activity, and minimize duplication of effort—on matters pertaining to Data Governance in Canada.**

Data Governance standards refer to best practices that guide the collection, usage, storage, archiving, transfer and disposal of Data. The DGSC's roadmap is being drafted by 4 cross-sector working groups and will describe the current and desired state of Data Governance in Canada. The roadmap will also identify gaps, make recommendations to fill the gaps, establish priorities for action, and suggest organizations that will eventually develop Data Governance standards.

What is this survey about?

There is a long history of poor data collection and misuse of information collected about Indigenous populations in Canada. Currently, many First Nations, Inuit, Métis and other Indigenous groups and organisations are striving towards the concept of data sovereignty. Decisions on data governance standards, such as the DGSC's roadmap, cannot be made without the close involvement of Indigenous groups. **This survey is part of a preliminary study to identify Indigenous perspectives on data governance in Canada.**

In this phase, Firelight is reaching out to Indigenous organisations and experts across multiple regions and sectors in order to gain an initial understanding of:

- **What are the main data governance issues or challenges that Indigenous groups currently face?**
- What standards exist relating to Indigenous data governance?
- What is the ideal future scenario for Indigenous data governance?
- What role should data standards play in this scenario?
- How do we get there?
- Who should be involved?

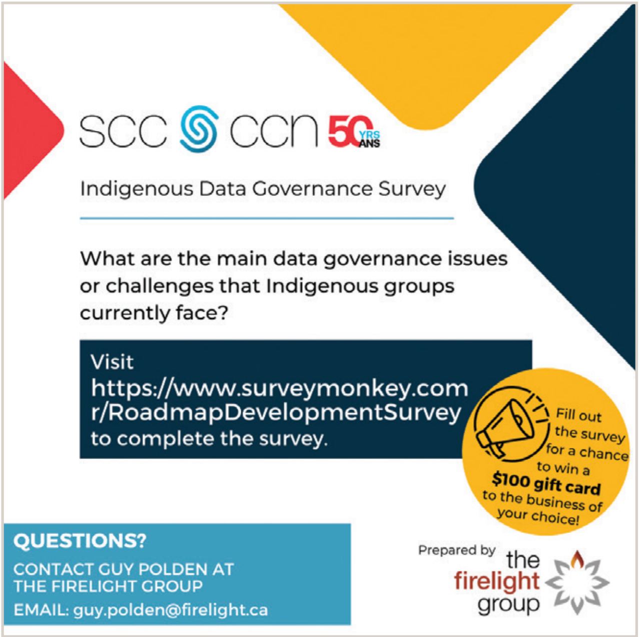
This survey will be followed by interviews with key experts in the field of Indigenous data governance across a wide variety of sectors. The information that you and other participants share in this survey will be used to develop a report on Indigenous Data Governance that will be submitted to the DGSC. This report will provide a series of recommendations based on the responses provided by participants, including how Indigenous groups could continue involvement in this process.

Visit
https:/www.surveymonkey.com/r/RoadmapDevelopmentSurvey
to complete the survey.

Fill out the survey for a chance to win a **$100 gift card** to the business of your choice!

Questions?
Contact Guy Polden at The Firelight Group
Email: guy.polden@firelight.ca

Prepared by the firelight group



SCC CCN 50 YRS ANS

Indigenous Data Governance Survey

What are the main data governance issues or challenges that Indigenous groups currently face?

Visit
https://www.surveymonkey.com
r/RoadmapDevelopmentSurvey
to complete the survey.

Fill out the survey for a chance to win a **$100 gift card** to the business of your choice!

QUESTIONS?
CONTACT GUY POLDEN AT
THE FIRELIGHT GROUP
EMAIL: guy.polden@firelight.ca

Prepared by the firelight group

Annex D —

Use Cases

wBackground

Recent initiatives have developed nationally in support of community health and the need for standardization. For example, the Community Health Workers Network of Canada has developed a Canada-wide initiative to support community health workers[21] and strengthen the development of community health nationally. As community health workers are "grounded in the communities they serve and responsive to the many challenges they face,"[22] it is important for the private and public sector to work together to develop a safe, secure and trusted environment for Canadian community health. Community health data needs to become a priority for policymakers, politicians and business leaders to bring community health policy into government, bridge gaps between the various health institutions – particularly as it relates to the interoperability of community health data and virtual health care delivery – and ensure that individuals from the various communities in Canada are accommodated.

COMMUNITY HEALTH DATA AND STANDARDIZATION

Health records and data in a data governance standardization context refers to the capturing and sharing of information with health care providers and allied partners. One of the unique aspects of health care is that data can be used for the benefit of the individual and the broader community. Balancing the needs of the individual and the needs of the community, although dependent on the health scenario, is the art of data governance in health. The Data Governance Standardization Collaborative, through its use case on community health data, looked at aspects of data governance involved in the distribution of health records and data to participants within the health system utilized by electronic health records (EHRs) as it relates to COVID-19.

[21] Community Health Network of Canada. https://www.chwnetwork.ca/index.php?option=com_content&view=article&id=27&Itemid=108

[22] Community Health Network of Canada. https://www.chwnetwork.ca/index.php?option=com_content&view=article&id=27&Itemid=108

Health records and data provide valuable information about the health of the population. There is a need to develop standardized health records across Canada as there are currently different standards for health care (e.g., vaccinations or diagnostic results) across the country. There are also inconsistent standards for capturing and sharing health information with other health care providers and allied partners. This is important given that the "the full value of digital health will be realized only when health information systems are connected and able to be easily accessed and shared… ."[23]

Health data standards are key to health interoperability. The development of pan-Canadian standards will provide technical language and clinical terminology to allow health care providers across the country to communicate and share health information in a safe, reliable and consistent manner. When used in digital health solutions, these standards: 1) support care team members to accurately interpret and exchange information needed for safe and effective care; 2) facilitate clinical decisions through alerts and reminders; and 3) enable data aggregation, with appropriate approvals, for clinical research, ultimately leading to better outcomes.[24]

The building of a single EHR to address health data inconsistencies would require all existing EHRs be reviewed to determine which is best to adopt, after stakeholder consultation (e.g., with health professionals and patients). Digital health records provide immense value to the health community as patients' health records, particularly those for visitors from other provinces, are often incomplete and inconsistent. This is a result of health care being a provincial responsibility, and as such there are different provincial standards for health records and data across Canada. This makes it very difficult for health care providers, allied partners and even in some cases patients to get a complete and clear medical history. The lack of timely access to information means patients are at risk of harm from incorrect diagnoses and avoidable side effects.[25]

Looking specifically at health records and data in terms of COVID-19, vaccinations for example are available to everyone and provide value for the individual in preventing illness and for the population in preventing outbreaks. Educators use vaccination as an entry criterion into their school system. The issues connected to the lack of standardization of health records has had a major impact on Canadians, such as within education systems where thousands of students have received notices to get their vaccinations updated and hundreds have been suspended pending the vaccinations being completed. When a vaccination for COVID-19 is a reality, this will be paramount.

The need for health records standardization, especially given the importance of health data, varies among the different actors of the health community. For example, public health actors look to health records to protect the health of the population; health policy makers look at health records to determine funding for effective vaccinations; education policy makers desire health records to keep their population safe; and private-sector agents look to health records to profit from the sale of effective vaccinations. Meanwhile, researchers use data to determine the effectiveness of, and make improvements to, such things as vaccinations and methods and tracing of outbreaks, and regulators use health data to provide protection of an individual's right to assert their ownership of data.

[23] https://www.infoway-inforoute.ca/en/solutions/clinical-interoperability-and-standards
[24] https://www.infoway-inforoute.ca/en/solutions/clinical-interoperability-and-standards
[25] https://www.cbc.ca/radio/whitecoat/a-national-electronic-health-record-for-all-canadians-1.4976932

To address the intersection points of data governance and health data for COVID-19, there is a need for the harmonization of health language, as well as interoperability across relevant systems. For example, the harmonization of language and interoperability of vaccination systems would allow for the understanding of health data, with respect to the knowledge of which vaccinations provide protection against particular diseases using particular drugs, across relevant systems. This would help act as a portal for health data and avoid complications when individuals move out of province, change primary care givers, etc. It is also important to consider the access, linking and privacy of health data in order to determine which actors have the right to access health data with consent and which actors have the right to access health data without consent. There is a need to consider the use of analytics on health data. Analytics has the potential to enable the broader health community to determine the effectiveness of given vaccines as well as determine their side effects. Actors in the health community must also consider whether health data should be used to nudge behaviour, such as using health data to distribute reminder notifications of what vaccinations to take when, and where they are available.

The development of interoperable EHRs will provide each Canadian with a secure, private and accessible record of their health history and care within the health system. Developing EHRs with a focus on interoperability will facilitate data sharing across health care delivery organizations and geographical areas, improve access to health services, and enhance the quality of care, patient safety and efficiency, saving the health care system time and money.[26]

Community Health Data Dialogue Sessions

On December 9, 11 and 14, 2020, SCC and the DGSC hosted a series of dialogue sessions with Canadians on the topic of community health data. Two sessions were held in English and one was held in French. They were attended by more than 23 participants from across the country, including government employees, representatives from data security companies, medical and healthcare associations and agencies, and strategic advisors.

Each session began with a brief presentation by SCC officials on the role of the DGSC, the importance of standards and the current state of health data in Canada. Participants were then invited to contribute to a conversation focused around two main areas of discussion:

- The **current state** of health data across Canada, including who can access it, what uses it has and where it is not being used; and,
- The **ideal future state** of health data in Canada, including what rules, regulations or standards are needed for a health data framework.

CURRENT STATE AND CHALLENGES

During an interactive whiteboard activity at the outset of the discussions, participants identified three key challenges facing health data in Canada:

1. Lack of data and terminology standards
2. Lack of integration among health care providers, including segregated information
3. Significant differences in provincial/territorial laws restricting data linkages.

[26] https://www.infoway-inforoute.ca/en/solutions/digital-health-foundation/electronic-health-records/interoperable-ehr

Following the whiteboard exercise, participants engaged in small breakout group discussions. Participants identified several barriers to accessing health data in Canada, including the non-digitization of patient records, the inability of patients to have access to or share their personal health records, and the lack of integration of data systems that makes it difficult for health care professionals to share what health data does exist digitally. There is a lack of standardization within the health care system when capturing health data, reducing the ability to use that data to monitor public health trends or the effectiveness of treatments and health policies. Patients are often unable to contribute health information they collect about themselves through new technologies such as smart watches, even as the lack of standards for those technologies calls into question the accuracy and usefulness of self-collected health data. It was agreed that most patients and health care professionals do not have a sufficient understanding of the existing rules governing health data in Canada, nor do those rules make it easy for patients to provide their informed consent for the sharing and use of their personal health information.

IDEAL FUTURE STATE

Participants want greater interoperability of health data across Canada so patients and health care professionals can have sharable, standardized and high-quality health data, and patients can more easily receive and be reimbursed for medical treatments outside their home province or territory. Patients should be able to access and control their own health data so it can be used wherever and whenever they need it and be able to share standardized health data they collect through new health technologies. There must be strong protections to keep health data secure and tamper proof, and any consent for sharing that data should be purpose driven, with a clear lifecycle for that consent. There should be more education for patients and health care professionals about current health data rules and increased standardization of those rules in the future. Participants want health data to be able to move seamlessly between systems, jurisdictions, providers and patients to allow for equitable care wherever someone lives in Canada.

DISCUSSIONS

Current State of Community Health Data

In the first half of **breakout group discussions**, participants were asked to provide their views on the current state of health data in Canada.

Q1.1: What is the current state for community health data (i.e., who can access it, what uses does it have, where is it not being used)?

Theme #1: Access to Data

Several participants highlighted existing barriers to accessing health data in Canada. It was pointed out that, in most cases, notes between doctors or between doctors and patients are done by hand, making it difficult to share or trace information. Patients do not have access to their health records from their family doctor or from specialists or other health care providers. This can be a particular problem when moving from one doctor to another, such as when a family doctor retires, or if seeking out-of-province health care or follow-up care in a patient’s home province after initial treatment in a different one.

Participants also pointed to the difficulties in sharing information between hospitals and private practices and clinics, or between public health and EMS data, with several noting there is a common misconception that data systems are connected when they are not. This lack of connectivity has become clearer during the COVID-19 pandemic, with different organizations using different digital solutions to collect and store data about possible contacts and infections, without a regulated system to share and use that information.

Another issue raised was uncertainty about who owns a patient's health data and what happens to that data if a patient is incapacitated or dies.

Concerns were expressed about the security of health data, with several participants noting that databases can be easily exposed or "hacked."

Theme #2: Point of Capture

There was considerable discussion about issues related to when and where health information is captured. It was noted that new technology, such as wearable devices (e.g., FitBits, smart watches), means health data is now being captured not just in the traditional health care ecosystem such as clinics and hospitals but by patients themselves. Many of these wearable devices have not been designed with security in mind and the data they collect are unregulated and non-standardized, calling into question the accuracy and usefulness of that data. Even if the self-collected data can be relied upon, participants noted it can be difficult to share that data with health care providers.

Within the traditional health care ecosystem, there is a lack of standardization when capturing health data, making it difficult to use that data to monitor public health trends or to measure the effectiveness of treatments and community health policies. As one participant said, "It would be nice to have more structure at the point of capture."

Theme #3: Privacy and Consent

Participants noted that Canada's legal framework regarding privacy is robust, giving the country one of the highest standards for consent in the world. Generally speaking, there are two types of consent for collection and use of personal data: opt in or opt out, and Canada has tended to operate on an "opt in" basis. That said, participants felt it can be difficult to implement privacy standards for health data, especially when there are no existing regulations for the secondary use of health data that is collected. Others noted that some consent forms are too long or difficult to understand, making it hard for patients to give informed consent for what will happen to the personal health data they provide, how long that consent will remain valid, or what happens to that consent when a patient is incapacitated or dies.

Additionally, new technologies and wearable devices that allow patients to collect their own health data can endanger the privacy of that information in the absence of robust security standards or clear consent protocols.

Q1.2: What rules, regulations, or standards currently exist, that you are aware of, to regulate health data?

Theme #4: Poorly Understood Rules

There was general agreement that most patients and health care professionals do not have a sufficient understanding of the existing rules governing health data in Canada, leaving people unsure about their obligations when it comes to collecting, storing and sharing that data. Some participants said they take cues from the European Union's General Data Protection Regulation (GDPR) or data protection rules that apply in the United States, but these tend to have been developed to govern private organizations, not the public sector. Participants agreed that existing rules vary in each of the provinces and territories, which can complicate the sharing of health data between jurisdictions. There is also a lack of clarity about the rules governing the collection and sharing of health data by wearable devices.

Future State of Community Health Data

In the second half of **breakout group discussions**, participants were asked to provide their views on the desired future state of health data in Canada.

Q2.1: What is the ideal future state of health data in Canada?

Theme #5: Interoperability

Interoperability was a common topic of discussion, specifically as it relates to the flow of data across systems, jurisdictions and borders, and the need to facilitate interoperability when updating health data systems. There was consensus that standards would allow for greater interoperability across the country, providing patients and health care professionals with sharable, standardized, high-quality health data. Many participants said they want a health ecosystem where trusted, consumable information is ubiquitously available to patients and authorized users at the point of care so their health care provider can have the best available and most up-to-date information. This would require digitizing information, including patient files currently in non-digital formats at doctors' offices, clinics and other health service delivery points.

Other participants noted that improved interoperability would simplify the health data system by allowing the provinces, territories and federal government to share relevant information and make it easier for patients to receive and be reimbursed for medical treatments outside their home province or territory.

Theme #6: Access to Data

Beyond general agreement that health care providers and allied partners should have much improved access to health data to improve patient care and outcomes, much of the discussion about access to health data related to the ability of patients to both access and control their own data so they can use it whenever they need it. As one participant noted, "Many Canadians do not have a family doctor. People need that data so they can receive care when they need it." Another said they believe patients in future will have the primary responsibility of managing their own health data.

Participants also want patients to have the ability to share the health data they collect through new health technologies (such as smart watches, fitness apps and heart rate monitors) with health care providers to ensure their information is as complete and up to date as possible. "There is a ton of information being collected by these devices that largely goes unused by doctors," noted one participant.

Theme #7: Security and Consent

The security and trustworthiness of health information was seen as essential to an effective health data system. That means strong protections to make it tamper proof and strict controls over who can access any or all of that data. One participant said patient consent to grant access to personal health data should be purpose driven, which would determine the lifecycle of that consent, and that consent should be explicit in order to create confidence in the system. It was noted that, while the private sector could be fined for breaking privacy rules, a similar system – and enforcement – is needed for the public sector in order to maintain trust in how governments and government agencies use health data. "Canadians need to know what's happening to their data and have some say over it," said one participant.

Although participants generally felt it should be a patient's choice to share (or not to share) their health data, there was some discussion about whether the focus was too much on data privacy and not enough on risk management. One person wondered whether privacy could sometimes be sacrificed for the greater good, as the central purpose of using health data should be to improve the well-being of Canadians, both individually and as part of a wider community.

Theme #8: Education and Certification

Having noted earlier in the consultation that most patients and health care professionals do not have a sufficient understanding of the existing rules governing health data in Canada, there was agreement that there should be more education about those rules and increased standardization of rules in the future. It was pointed out that standardization does not stifle innovation, with many other professions, including engineering, having standardized rules that everyone must follow, and that those rules can evolve and change over time. One suggestion was that, once health data standards have been agreed to, there should be a mandatory course on them in colleges and universities. Another participant suggested there should be incentives for health care professionals to always stay up to date on health data standards, perhaps as part of their ongoing certification.

Q2.2: What is the ideal future state of health data in Canada?

Theme #9: A Unified Vision

Participants emphasized that the development of health data standards should always be done in a way that puts people at the centre of those efforts. The health care system should be simplified so provinces and territories can easily exchange information with each other and with the federal government. There should be a shared vision of interoperability of health data across Canada, with data moving seamlessly between systems, jurisdictions, providers and patients to allow for equitable care no matter where someone lives. It was suggested that the Canada Health Infoway and similar bodies could help to drive this unified vision and strategy and promote the adoption of pan-Canadian health data standards. Another suggestion was for Canada to adopt a data and information governance framework such as the one adopted by the Canadian Institute for Health Information. It was felt that a regulatory or standardization pathway would increase patients' confidence in the use of their personal health data.

Use Case Working Group Report

APPROACH

The Community Health Data use case group took a top-down view of the key issues each of the DGSC working groups were responsible for. The group was inspired by the work of Statistics Canada establishing their CODAS platform (to collect data from multiple sources and render it available for StatsCan and external use) and CIHI's Health Data and information Governance Framework (https://www.cihi.ca/en/health-data-and-information-governance-and-capability-framework). During the lifecycle discussions, several recurring challenges were identified and categorized into three themes.

The group quickly noticed that this use case applies well beyond COVID-19 and should consider the entire data supply chain i.e. the benefits of standardization when collecting and coding data at point of origin; how data exchange and interoperability assists with the aggregation of data; and guidance on analytics and insights that includes ethics and transparency, which can then drive action. A generalized data flow was developed to depict development of insights for community health (which involves individuals, health providers, researchers and policy makers). A structure for a data policy architecture was created aligned with the end-to-end data supply chain (included at end of this report).

The issues identified across the working group were mapped to the data policy architecture to identify potential overlaps and blind spots. The group reviewed each issue in turn and developed commentary and recommendations for consideration by the DGSC as a whole. These are presented below and divided into blind spots and refinements. The group has attempted to be general; however, some challenges may only be applicable to health.

To facilitate understanding and addressing the noted blind spots and recommendations, a brief description of the relevance to the Community Health use case is included with each item.

GENERAL FINDINGS

There is value in a common lexicon for the issues and DGSC should make sure the same terms are used consistently across all issues to avoid confusion and to simplify sharing of standards.

This includes:

- Roles (such as data owner, data custodian, data user, data steward).
- Perspectives (such as data provider, intermediary, consumer)

When developing standards, it will be important to clarify the role(s) involved and from whose perspective the standard applies.

Recommendation: The DGSC should review these findings and determine whether it makes sense to consolidate these items with existing issues or if a new issue should be created.

By adopting a top-down approach for data governance, the working group was able to identify several areas that could be blind spots.

- **Overall purpose, funding, and evaluation:** A data governance structure needs to have an articulated purpose and associated funding model and be established as a clear program of work. Further, a data governance solution should be monitored and evaluated for effectiveness. Standards may exist in particular for methods of evaluation.

  Relevance to Community Health: Health is delivered by multiple independent organizations that must work together, so coordination is essential. In addition, funding is necessary to coordinate. Without direction and funding, organizations will work independently, often weakening the end-to-end supply chain.

- **Monitoring, audit, and compliance:** A data governance program should have some practice around monitoring, audit, compliance and associated reporting to an executive oversight body.

  Relevance to Community Health: Similar to having a common purpose, there need to be methods to monitor compliance along the health data supply chain to enable trust with each other and with stakeholders.

- **Indigenous data management:** There are specialized requirements for the management of Indigenous data (e.g., aligning to OCAP principles for First Nations' data). This may be extended to management of other specialized ethno-cultural groups.

  Relevance to Community Health: Misuse of personal health information (PHI) is among the most visible ways in which Indigenous populations have been impacted. Visibly embedding principles that respect Indigenous data is crucial for reconciliation.

- **Stakeholder management:** There are many groups that are involved in end-to-end data lifecycles and should be involved in design and decision-making across data collection, storage and use.

  Relevance to Community Health: Similar to the previous point on Indigenous data, the public has expressed its concern about appropriate use of PHI. As we design our health data supply chains, understanding requirements to be trustworthy and involving stakeholders to demonstrate that trustworthiness will be critical.

- **Data sovereignty:** Laws and guidance for data held in Canada (and specific jurisdictions in Canada) have some variance, as do laws for Canadian data held or flowing through other countries. This is particularly important for intellectual property (IP) generated in other countries using Canadian data and understanding our collective rights.

  Relevance to Community Health: Health is projected to be one of the major growth industries in coming decades and so the creation and protection of IP is crucial. In particular, as data flows between countries, ensuring that we protect our Canadian data for our health systems will benefit everyone.

- **Data de-identification and re-identification:** A key method of risk mitigation for data sharing and use is data de-identification, wherein there could be protocols for purposeful re-identification where appropriate. A group (CANON – Canadian Anonymization Network) may be a good source of standards.

  Relevance to Community Health: As the use of PHI at an identifiable level brings with it great concerns, it is necessary to obfuscate the data to protect the privacy of individuals while maintaining sufficient detail to render the data meaningful for analysis. De-identification is the practices that achieves this. Furthermore, there are scenarios where re-identification is necessary for individual and public health.

- **Consent removal and its propagation:** The ability for a data owner to remove their consent should have clear guidance on how it can be done locally and along data supply chains (lineage).

  Relevance to Community Health: As health data moves across organizations to affect care for individuals and public health, it is necessary to understand how consent works (and where it is appropriate) across the life of a consent directive across all the places where the consent may be applied. For example, enabling broad-based personal consent may create data bias.

- **Preserving security:** A data supply chain is only as strong as its weakest link. As such, some concept of preserving security (and privacy) levels across partners would be appropriate.

  Relevance to Community Health: As health data flows across organizations, standards for security are more nuanced as it is done in the context of the organization and its outputs, as well as the context of the data itself.

- **Use of cloud technologies:** Given the proliferation of use of cloud technologies, adoption of standards for data in cloud use – in particular the rights and obligations of involved organizations – may be appropriate.

  Relevance to Community Health: Like most industries, there is a significant uptake of use of the cloud – public or private – for health services. As more data is available in the cloud, the risks of re-identification increase.

- **Vendor contracts:** Technology companies are engaged to support business operations and often enable data flow within and between organizations. Many vendor contracts are not designed considering the end-to-end data supply chain. There could be benefit in identifying best practices and standards that could be broadly adopted.

  Relevance to Community Health: Most health technology is purchased (rather than built), necessitating the procurement of technologies from vendors. Often these vendor contracts are negotiated by non-experts (e.g., sole primary care providers), which has led to contracts that are not in the best interest of health systems. Having standard expectation around vendor contracts that ensure the free flow of data will be beneficial. This is the implementation of some principles from GDPR (right to transfer).

- **Open API protocols:** It may be useful to establish open API standards (such as use of HL7/FHIR for health data) to facilitate the flow of data within and between organizations along data supply chains.

  Relevance to Community Health: Similar to the previous point, for health data to generate greater value for Canadians, clearly defining the protocols under which data is transferred will simplify the tools needed by other technology companies and innovators to use the data. Several other countries have already adopted this concept (notably UK and USA) – using standards like HL7/FHIR and SNOMED.

- **Data content standard management and stewardship:** The processes to manage data content standards over the data lifecycle are not well defined and communicated, in particular when it involves multiple organizations across a data supply chain. Groups like the IEEE and ISO could have guidance on how standards are managed, shared and changed.

  Relevance to Community Health: The scope of data in health is vast, with few content standards universally adopted across Canada. Clearly defining the processes through which standards are developed, communicated and managed will help clarify what accountability needs to exist.

- **Guidance on minimum data sets/core data elements:** Many data standards across organizations are defined by a 'minimum data set' or set of 'core data elements' that, when agreed, facilitate the sharing and trusted use of that data.

  Relevance to Community Health: Similar to the previous point, clarifying processes for development, communication and management of minimum data sets will help clarify what the accountability looks like to motivate action to establish what needs to exist.

- **Use of forms and unstructured data:** Some highly valuable data is captured in an unstructured way. Some guidance may be useful to find the balance between the use of forms and unstructured data, in particular with an overlay of use of machine learning tools.

  Relevance to Community Health: Health data is vast. Much of it is structured; however, there is significant richness in unstructured doctor notes which are difficult to mine for insights. Having some clear guidance and standards for the mix of using forms and unstructured data would be useful, in a way that aligns with practice workflows and assists achieving desired outcomes.

- **Master data management:** While most data content standards are industry specific, the concept of master data management and the ability to link data sets together is critical, in particular across data supply chains.

  Relevance to Community Health: In order to derive key insights for health data, it is beneficial to be able to link data sets together – and that often requires clear master data that is broadly adopted (either physically or logically). Further, the master data may have associated data that means the data can be collected once and used many times (such as the address or race/ethnicity of an individual).

- **Analytic code of conduct:** In addition to the idea of an ethical code of conduct, it may be beneficial to establish a standard checklist for the appropriate generation and sharing of insights that establishes an analytics' trustworthiness.

  Relevance to Community Health: Analytics in health are growing significantly. As the ability for anyone to generate insights expands, the ability to misuse the data also expands. Having a common code of conduct for health insights would help build trust in the analytics for policy makers and the public.

Recommendation: The DGSC should review these findings and determine whether it makes sense to consolidate these items with existing issues or if a new issue should be created.

CONSOLIDATIONS AND REFINEMENTS

By reviewing identified issues across working groups in the context of the identified use case, this group was able to identify some opportunities for consolidation of common items across issues. Further, by doing that consolidation, it allows for refinement of some of the issues into a package that could be easier to address by way of standards analysis.

The findings in this section are presented by issue. The major issue is bolded. Sub-issues proposed to be consolidated are included under the major issue. The rationale for the relevance of the item and proposed changes for Community Health are noted.

Issue 1 Accountability Framework: This should be divided into three parts:

a. To data owner (gaining consent, transferring, revoking)

b. Within organization (who does what)

c. Across organizations (in a data supply chain)

- **Rationale:** Health happens in the context of a data supply chain, so accountability needs to be considered locally, in the context of interaction with upstream/downstream partners and the overall data flow and desired outcomes.
- Issue 5 Management Governance could be merged with (b) above

  a. Local legislation should be included with PIPEDA

  b. Possibility to align to Digital Charter
- Issue 24 Trusted Data Intermediaries could be merged with (b) above

  a. Data intermediaries are a type of data organization
- Issue 8 Harmonization and Interoperability of Data Practices/Open Data could be merged with (b) above

  a. Data policies are how accountabilities are defined

Issue 30 Technical Elements of AI Solutions: Note that the ISO is working on a related standard currently.

- Suggest this item be focused on the generation of algorithms rather than the reports that are produced and used (Issue 33 Interpretability and Explainability of AI Systems)
- **Rationale:** Analytics in health – and specifically the use of AI – is growing significantly. While AI solutions will generate reports, the higher-value deliverable is in the creation of algorithms. These can be implemented in point-of-care solutions to assist with diagnostics or in development of evidence-based policy.
- Issue 35 Performance Management Systems for Analytics and AI Systems could have parts merged in here with that focus
- Issue 33 Interpretability and Explainability of AI Systems could have parts merged in here with that focus

Issue 2 Certification for Professional Roles: This standard should focus on the process of certification rather than certification itself. Organizations like ARMA may provide useful insights.

- **Rationale:** There are several organizations in Canada that provide some certification for using data (notably CHIMA and Digital Health Canada). The proliferation of certifications may continue, so establishing criteria for what certification does – perhaps leveraging these models – could be useful.
- Issue 3 Digital Literacy could be merged with issue 2 Certification of Professional Roles, depending on what the audience for ‘digital literacy’ would be. Item could talk to level of knowledge/capability for various levels of an organization.

Issue 20 Data Access: Consideration to include language for necessary and proportionate data access.

- **Rationale:** Privacy is often considered a barrier for accessing health data, due to a low risk tolerance enacted by privacy officers. Adopting more nuanced approaches that leverage consideration for ethics will be beneficial. This is being championed by Statistics Canada in its data strategy.
- Issue 22 Identity Management – Validation and Authentication and Issue 25 Authorization for Data Collection and Sharing could be merged into Issue 20 Data Access to include the parts of the end-to-end access process.

Issue 11 Data Collection: There are several issues that collectively talk about data lifecycle management in the context of an organization. These could be consolidated.

- Note that some items in data collection are addressed in blind spots above (notably forms and vendor contracts)
- Across these items, some additional information could be included on:
  a. Data retrieval (as part of retention – Issue 21)
  b. Data portability (as part of Issue 29)
- **Rationale:** There will be more channels through which health data is generated and collected; these will need to be integrated with legacy health data supply chains.
- Issue 21 Data Retention could be merged, or kept separate with retrieval
- Issue 23 Data Sharing, Exchanging and Integration could be merged into the group or with Issue 29 Data Portability and Mobility
- Issue 12 Data Systems Management could be merged into the group
- Issue 29 Data Portability and Mobility could be merged into the group or with Issue 23 Data Sharing, Exchanging and Integration

Issue 6 Data Privacy: The issue description focuses on data ownership and rights whereas it could focus on a more extensive view of data privacy, including considerations for Privacy Impact Assessments, Data Sharing Agreements, and training of staff.

- **Rationale:** Privacy is critical for PHI and the subject of health-specific legislation across the country. It extends well beyond data ownership and rights to using the data under various contexts and forms. While Privacy by Design is a standard that has been applied, it has been extended in other jurisdictions (notably in the UK with its Caldicott Principles).

Issue 31 Data Value Chain: Suggest this requires more content to help establish standard. Focus should be on intellectual property and sharing of value with original data owners (example – in the Netherlands, pharmaceutical companies receive data from governments in exchange for funding parts of their health system).

- **Rationale:** Health rests on the effective operation of data supply chains. Those generating value at the end of data supply (though IP generation) may have some obligation to share with the chain that led to the creation of the IP.

Issue 26 (Transparency and Communication of Data Analytics): Consider split of Issue 26 into:

a. Ethics, Transparency and Communication to Data Owner

b. Ethics, Transparency and Communication to Analytic User

- The issue focuses on (a); however, there are risks associated with (b)
- Note that Edward Tufte has written significantly on the dangers of unaccountable analytics. May be suitable to define 'code of ethics for analytics'
- Note that the risk of data enrichment (linking) increases the risk of re-identification. Could make mention of emerging techniques (homomorphic encryption)
- In particular, there could be value in standards around transparency of communication to avoid analytics that sound the same but are not (e.g., positive COVID-19 test counts were measured differently in various parts of the country)
- May be worthwhile to look up standards related to data trusts, data collaboratives or data commons
- **Rationale:** As analytics proliferate in health, it is essential that transparency exists to build trust among stakeholders. There are more nuances in health due to the use of PHI to generate the insights and the potential for the analytics to create harm to individuals, in particular for marginalized groups (e.g., insurance rates increasing significantly for those with genetic pre-conditions).

Issue 13 Discoverability of the Data: Propose to limit scope of issue to catalogue/inventory as otherwise there is overlap with Issue 20 Data Access

- This would include statements of the quality, integrity and traceability of the data without covering how quality is achieved (Issue 18 Data Quality and Fitness for Use Assessment).
- **Rationale**: With the vastness of health data with many collection and aggregation points, it is hard for health organizations to know who has what data over what period of time. Improving discoverability – along with understanding its fitness – is important for improving speed and trust.
- As a group, this would cover several related issues
- Issue 16 Metadata Management could be merged into the group
- Issue 28 Data Transparency, Lineage and Traceability would be merged into the group
- Issue 15 Manual Tagging of Data would be merged into the group

Issue 18 Data Quality and Fitness of Use Assessment: Should be merged as a bucket of items determining level of data quality, which is a statement about the fitness of the data

- Note that 'quality' of data can usually only be determined at point of origination, whereas other checks are determining conformance of the data to allowed patterns.
- May be useful to expand definition of Data Quality to Information Quality as a broader concept of the quality of insights produced. Statistics Canada has Quality Guidelines that could be useful.
- **Rationale:** Given the vastness and complexity of health data flows along the data supply chain, it is important to assert fitness of data for the analytics that are produced which balances timeliness of the outputs and the quality of the data utilized.
- Issue 18 Data Quality and Fitness for Use Assessment would be merged into the group

Issue 33 Interpretability and Explainability of AI Systems: Suggest that this item be focused on applying AI algorithms and using insights

- This could also be made more generic as explainability of statistical algorithms (including AI), as not all algorithms are generated by AI but all should be explainable.
- **Rationale:** As analytics and use of AI proliferate in health, the ability to trust the results will be essential. That will require the ability to explain how the algorithm works to establish that trust.
- Issue 35 Performance Management Systems for Analytics and AI Systems should be merged into this group

Issue 9 Data Actor and Data Transaction Roles: Suggest this is replaced with lexicon above rather than being a 'standard'

- **Rationale:** Data roles exist along health data supply chains and should be defined in a preamble, then used broadly through the other standards.

Issue 34 Assessment and Management of Bias: This could be merged with the blind spot for a checklist for analytics (above)

- Part of bias is transparency and part is awareness. Having a conscious way to bring the unconscious (bias) forward may be effective
- **Rationale:** Given the vastness of health data, the likelihood for inherent bias in that data – based on prior historical norms – is higher. Standards to measure and manage that bias are essential to establish trust.

Issue 17 Organizational Data Policy Strategies and Risk Management: This covers many areas that could be covered under other issues (such as Issue 20 Data Access, Issue 6 Data Privacy, and Issue 32 Transparency and Communication of Data Analytics).

- Could focus on how these individual issues are brought together under a program of risk management that is optimizing positive outcomes while minimizing negative impacts.
- **Rationale:** Mobilizing health data requires coordination across many organizations having a level of consistency in their policy to generate collective outcomes. That consistency is aided by a common approach to risk management that balances privacy, access and ethics.

Issue 27 Management of Ontologies: Propose to expand the definition of this to explicitly build standards for master data and hierarchy management

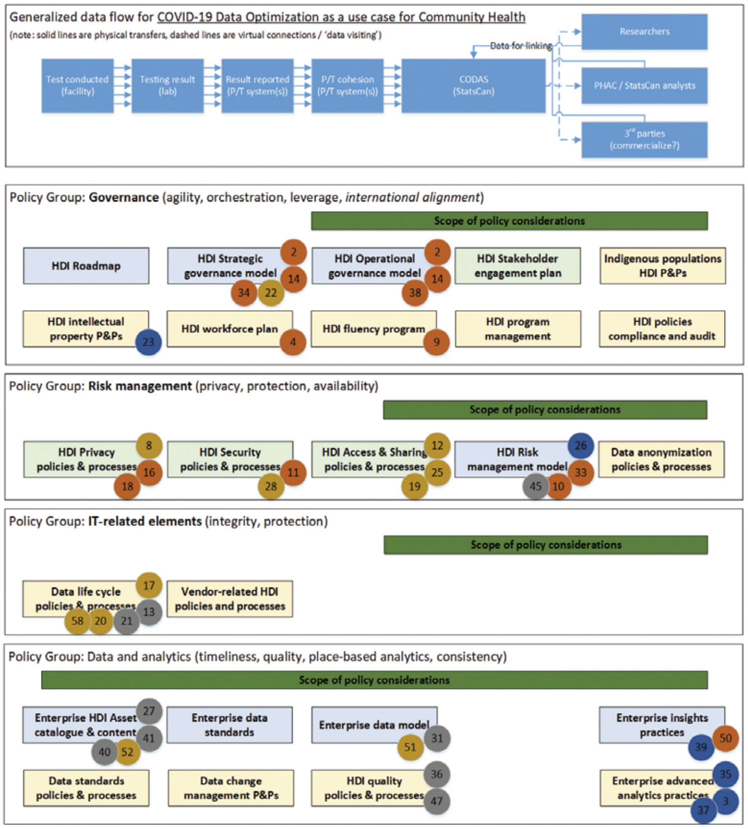
- **Rationale:** As health data is vast, there is need for some common ontologies to enable the effective flow of data across health data supply chains that supports linking of the data to generate more utility and insights. Useful reference could be EHDEN (in Europe) and its use of OHDSI (Observational Health Data Sciences and Infomatics).
- Issue 14 Data Linkage would be merged into the group

Recommendation: The DGSC should review these findings and determine whether it makes sense to consolidate these items with existing issues or if a new issue should be created.

CONCLUDING COMMENTS

The diversity and complexity of health care makes standardization challenging. While standardization could help to ensure the security of individuals' data while also helping to bring efficiencies into the management of data, there is a complex regulatory environment that oversees health data. This adds a challenge when looking at exploring innovation in data flows.

The working group appreciates the opportunity to have been asked to do this review. Through their work and feedback from the public consultations, a list of recommendations was identified for consideration for the DGSC.


Generalized data flow for COVID-19 Data Optimization as a use case for Community Health
(note: solid lines are physical transfers, dashed lines are virtual connections / 'data visiting')
Test conducted (facility)
Testing result (lab)
Result reported (P/T system(s))
P/T cohesion (P/T system(s))
CODAS (StatsCan)
Data for linking
Researchers
PHAC / StatsCan analysts
3rd parties (commercialize?)
Policy Group: Governance (agility, orchestration, leverage, international alignment)
Scope of policy considerations
HDI Roadmap
HDI Strategic governance model
2
14
34
22
HDI Operational governance model
2
14
38
HDI Stakeholder engagement plan
Indigenous populations HDI P&Ps
HDI intellectual property P&Ps
23
HDI workforce plan
4
HDI fluency program
9
HDI program management
HDI policies compliance and audit
Policy Group: Risk management (privacy, protection, availability)
Scope of policy considerations
HDI Privacy policies & processes
8
16
18
HDI Security policies & processes
11
28
HDI Access & Sharing policies & processes
12
25
19
HDI Risk management model
26
33
45
10
Data anonymization policies & processes
Policy Group: IT-related elements (integrity, protection)
Scope of policy considerations
Data life cycle policies & processes
17
13
58
20
21
Vendor-related HDI policies and processes
Policy Group: Data and analytics (timeliness, quality, place-based analytics, consistency)
Scope of policy considerations
Enterprise HDI Asset catalogue & content
27
41
40
52
Enterprise data standards
Enterprise data model
51
31
Enterprise insights practices
50
39
Data standards policies & processes
Data change management P&Ps
HDI quality policies & processes
36
47
Enterprise advanced analytics practices
35
3
37

Working Group Issues:

Working Group

1 2 3 4

WG1:

2. Accountability framework
4. Certification for professional roles
9. Digital literacy (and open data)
10. Data Risk and liability management
11. Cybersecurity protection
14. Data governance management
16. Privacy (data rights)
18. Data rights
33. Guidance on trustworthiness ethical and societal use of data
34. Harmonization of interoperability of data practices
38. Data actor and data transaction roles
50. Secondary use of data

WG2:

13. Data Collection (at point of origination)
21. Data system management
27. Discoverability of data
31. Data linkage
36. Methods to determine fitness for use
40. Manual tagging of data
41. Meta data management
45. Organizational data policy strategies and risk management
47. Data Quality

WG3:

8. Consent management
12. Data access
17. Data retention
19. Identity management – validation and authentication
20. Data sharing, exchanging, and integration
22. Data intermediaries
25. Disclosure and consent for data collection and sharing
28. Encryption
51. Management of ontologies
52. Data tagging, lineage, and traceability
58. Data portability and mobility

WG4:

3. Technology elements of AI solutions
23. Data Value Chain (monetization)
26. Disclosure & communication of risks for data owner
35. Performance management systems for placement, depth, etc.
37. Interpretability of algorithms
39. Assessment and management of bias

Policy Group: **Governance**
- Objective (scope: policy / research / both)
- Governance (decision rights on design)
- Value creation and sharing (for who)
- Accountability (across data supply, who does what)
- Control (project control audit and monitoring)
- Engagement (public, provider, policymaker, others)

Policy Group: **Risk management**
- Principles of risk management (balanced in ethics)
- Requirements to get access to source
- Privacy requirements at rest
- Security requirements at rest and in motion
- Requirements for users to submit query / access results

Policy Group: **IT-related elements**
- Guidance on retention of data / logs
- Design of end-to-end data supply chain
- Standards for data exchange
- Engagement with vendors to embed requirements

Policy Group: **Data and analytics**
- Minimum data set for data query
- Enterprise data standards with mapping to local context
- Template for data catalogue, inventory, dictionary
- Design of data quality, conformance, and remediation
- Approach to Indigenous populations' data
- Analytic practices (including considerations for AI)

Use Case #2 – Digital Identify and Open Banking

Background

In the age of COVID, in-person interactions have become restricted, so operating in a digital context is becoming increasingly important for Canadians. Open banking (or Consumer-Directed Finance) is a prime example of this. Digital connectivity, data and consumer needs are driving institutions, governments and Canadians towards third-party arrangements. However, lack of regulation and standards to support this new sector, and tools to enable this, such as digital ID, are leaving Canadians behind – economically, competitively and, most importantly, with regards to security.

Government and industry collaboration on this issue is essential, with more than 70% of Canadians wanting the public and private sectors to work together on a joint digital ID framework.

Various national initiatives have been established over the last two years in support of digital identity, open banking and the need for standardization. For example, in 2018, Canada joined a network of countries looking to use digital technologies to benefit citizens. One element of this strategy is developing a trusted Digital ID platform.[27] Open Banking was also identified by the Senate Committee on Banking, Trade and Commerce as one of the key use cases that should be addressed by the Data Governance Standardization Collaborative (DGSC).[28] In 2019, the Department of Finance appointed an Advisory Committee to review the merits of Open Banking. Most importantly, "consumers, businesses and government entities [must] work together to achieve the common goal of enabling a safe, secure, and trusted ecosystem for Canadian digital identity."[29] Digital ID needs to be a top priority for policymakers, politicians and business leaders, in order to bring digital ID policy into government, adjust language in the policy to accommodate for trusted digital ID, and incentivize businesses to explore digital solutions in their organizations. Government and industry collaboration is essential, with more than 70% of Canadians wanting the public and private sectors to work together on a joint digital ID framework. Additionally, 83% of Canadians trust government to keep their data safe and 81% trust financial institutions.[30]

DIGITAL IDENTIFICATION, OPEN BANKING, AND STANDARDIZATION

In some countries, digital ID is the connective tissue between financial data sharing, innovative financial solutions and security. For example, Australia recently announced an investment of AUD $256.6 million (about CAD $243 million) into a digital identity system as part of an economic recovery plan in response to COVID.[31] Unfortunately, Canada is falling behind. While 2019 brought the "Merits of Open Banking" consultation by the Department of Finance in addition to the Canadian Digital Charter, we are still behind in linking our government identification with our online credentials, which we need to do to provide secure, convenient open banking frameworks. According to a McKinsey study, on average, full digital ID could unlock economic value equivalent of 3% to 6% of GDP in 2030,[32] or about CAD $48 billion-$97 billion.

[27] Susan Crutchlow, TransUnion. Digital Identity – A Key Driver of Canada's Digital Economy. https://www.transunion.ca/blog/digital-identity.

[28] Report of the Standing Senate Committee on Banking, Trade and Commerce. Open Banking: What it means for you. https://www.sencanada.ca/en/info-page/parl-42-1/banc-open-banking/.

[29] DIACC. The Economic Impact of Digital Identity in Canada. https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.

[30] DIACC. Canadians are Ready to Embrace Digital Identity. https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/.

[31] Prime Minister of Australia. Digital Business Plan to Drive Australia's Economic Recovery. https://www.pm.gov.au/media/digital-business-plan-drive-australias-economic-recovery.

[32] McKinsey Global Institute. Digital Identification: A Key to Inclusive Growth. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

A form of digital ID is already in place and used by governments, financial institutions and fintech companies (i.e., accessing Service Canada or Canada Revenue Agency, filing taxes online, or online banking). However, in the absence of a Canadian identity management framework supported by robust standardization and regulation, there are challenges in the way that Digital ID works today in Canada. Online identities are fragmented across many business/entities, which increases the systemic risk of fraud through accumulating data. Data breaches occur and erode people's confidence in that organization and the digital economy.[33] Identity has traditionally been proven using physical records such as passports or identity cards. Unfortunately, physical documents can be forged or altered, and fraud accounts for significant financial losses. In addition, many Canadians do not have sufficient means to prove their identity, resulting in them being excluded from convenient digital access to services such as healthcare, government and banking. This has never been more apparent than during these difficult times.

Canadians want more control and agile access over their data, and this makes economic sense. Millions of Canadians are already sharing banking information with third-party providers; however, due to a lack of a formal Open Banking regime, they are forced to rely on insecure methods such as screen-scraping, putting their personal identity and sensitive financial information at risk. With a Canadian digital identity framework, there are "potential net savings per institution at or above CAD $100 million per year, through operational efficiencies… and reducing fraud."[34] With these challenges in mind, standardization can be a possible solution for implementing a Canadian Digital Identity framework, reflecting values that Canadians support (inclusion, transparency, trust).

Digital ID and Open Banking Dialogue Sessions

On December 2, 3 and 4, 2020, SCC and the DGSC hosted a series of dialogue sessions with Canadians on the topics of digital ID and Open Banking. Two of the sessions were held in English, while the third was held in French. The sessions were attended by more than 100 participants from across the country, including representatives from financial institutions and third-party service providers.

Each session began with a brief presentation by SCC officials on the role of the DGSC, the importance of standards, and the current state of digital identity and Open Banking in Canada. Participants were then invited to contribute to a conversation focused around two main areas of discussion, namely:

- the current situation of digital ID and Open Banking in Canada, including existing challenges, opportunities, rules and standards; and,
- the ideal future state, from the desired benefits for consumers to the laws and regulations needed for effective digital ID and Open Banking frameworks.

CURRENT STATE AND CHALLENGES

During an interactive whiteboard activity at the outset of the discussions, participants shared their perspectives on the challenges facing digital ID and Open Banking in Canada. Ultimately, four recurring and overarching challenges emerged:

1. Trust, and the need to earn and maintain the confidence of consumers
2. Security, and the need to manage risk, protect privacy and prevent fraud
3. Fragmentation, and the need to optimize cooperation, interoperability and efficiency
4. Effective governance and oversight, and the need for consistent rules, regulations and standards that are aligned across jurisdictions

[33] DIACC. The Economic Impact of Digital Identity in Canada. https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.
[34] DIACC. Industry Insights: Digital ID in Financial Services. https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.

Following the whiteboard exercise, participants engaged in small breakout group discussions. When reflecting on the current state of digital ID and Open Banking, participants generally felt that Canada is extremely well-positioned to become a front-runner in both areas; however, there was also agreement that we are falling behind other countries in developing the necessary legal and regulatory frameworks. Multiple participants noted that more leadership and support is needed from the federal government as there are currently no laws to enable and govern Open Banking in Canada. Consumer awareness and education was another gap identified by participants, who said Canadians lack the understanding needed to use and trust digital ID and Open Banking systems. However, it was also noted that there is a shared onus on governments and industry to ensure that individuals are aware and confident in Open Banking.

IDEAL FUTURE STATE

When looking ahead to the desired future state of digital ID and Open Banking, participants generally agreed that the individual consumer should have greater control and decision-making power when it comes to who has access to their personal data and how it is used. This, participants felt, would require a fundamental paradigm shift from institutional data ownership and control to a more transparent and democratic consumer-centric model. Participants envisioned a comprehensive and trustworthy national digital ID system that works seamlessly across national and provincial levels, and they underscored that broad participation and interoperability, together with strong privacy protections, are critical to success.

DISCUSSIONS

Current State of Digital ID and Open Banking

In the first half of **breakout group discussions**, participants were asked to provide their views on the current state of digital ID and Open Banking in Canada.

Recurring themes and key insights from the discussions are summarized below.

Q1.1: What is the current situation for digital ID and Open Banking (i.e., what information is required, how secure is the information, who has access)?

Theme #1: Canada is well-positioned to implement digital ID and Open Banking frameworks but continues to lag behind other countries.

Some participants said that Canada is extremely well-positioned to adapt and take advantage of emerging technologies and digital solutions and to become a leader in the areas of digital ID and Open Banking. It was noted that Canada has unique insights and knowledge to draw upon, particularly from its world-class financial services and tech sectors. One participant gave an analogy to explain Canada's current situation: "It's like we have running shoes, but we're just not putting them on yet." Multiple participants noted that more leadership and support is needed from the federal government as there are currently no laws to enable and govern Open Banking in Canada.

There was consensus across all groups that Canada is falling behind other countries in developing digital ID and Open Banking capabilities. It was noted that many international players are far ahead of Canada in terms of both technology and regulation. International jurisdictions like the United Kingdom, Australia and Hong Kong were noted as key players who are "years ahead" of where Canada is today. A key question asked during these sessions was: "What learnings can we gain from successful global infrastructure? We have to be conscious about the excellence around the world and adopt or implement best practices."

Believing that time is of the essence, some participants suggested Canada should avoid getting bogged down by "reinventing the wheel." One participant said: "We're so far behind. Let's just get started with something. We have to find a good balance between doing the right thing and doing it perfectly."

Several participants noted that, in Canada, we are still reliant on paper-based systems when it comes to banking and identification, and there is a need to continue transitioning to digital solutions. For example, one participant noted that to open a bank account they have to physically go into the bank to produce several documents. They acknowledged that this seems to be changing little by little, but rules vary from bank to bank. Participants posited that if we can standardize credentials such as a passport, driver's licence, etc. in a digital format, this would help to support interoperability.

Theme #2: Limited consumer awareness and understanding of digital ID and Open Banking.

It was noted that there is a current lack of awareness and understanding among Canadians about digital ID and Open Banking. Participants identified the need to explain the concepts in a simple, clear way, to achieve a fundamental level of trust among the Canadian public. When it comes to data sharing and data retention, multiple participants emphasized that understanding what data will be kept, for how long and for what purpose, is key to Canadian consumers' participation and having confidence in third parties. It was also noted in one of the sessions that there should be more cybersecurity and digital ID education in the school system.

The topic of privacy and security risks was also top-of-mind for participants, especially as those risks pertain to individuals and their personal and banking information. It was suggested that "oversharing" happens when trying to open a new bank account and there is concern around what the banks are doing with that information. Some participants were worried that consumers might be blind to these risks.

STANDARDIZATION PAIN POINTS

- Competition is a driver for so many things – as long as open banking is in place in a non-structured way. Standards might be used to entrench market power or build barriers. Standards should be consumer driven.
- Consent processes are too complex and technical for the average Canadian to understand and to make an informed decision when sharing their data.
- Part of the confusion with standardizing is how all these things are interoperable between sectors and digitally.
- Information needs to be explained in plain language for the consumer.
- There are services today that are being offered that Canadians are lending themselves to with no regards to the security. It is more about convenience than security. Guardrails need to be put in place.
- Every information custodian can set their own standards. We need to move away from knowledge-based access to information/authentication. We have to focus on principles to move together faster. To move forward, we must empower those trust custodians.
- When we look to standards and policies, how do we mitigate the risk of certain segments of Canadian society who are not able to participate in a digital identity and transactions, or who do not wish to participate – what do standards look like for them?

Q1.2: What rules, regulations, or standards currently exist, that you are aware of, to regulate digital ID and Open Banking?

Theme #3: Several other countries have implemented rules, but approaches vary and lack consistency.

Participants mentioned various standards implemented by a number of different countries. Noting a divergence in approaches, some participants said it would be beneficial to work towards establishing common international standards (e.g., between Canada and the UK) in order to facilitate international business and mobility, among other things.

Some examples of existing standards include:

- Estonia digitizing government services for over a decade
- Hong Kong Monetary Authority's Open Application Programming Interface (API) for the banking sector
- UK Open Banking standards and moving to open finance
- Open Banking initiatives in Australia, New Zealand and Mexico, with a less top-down approach

Theme #4: Rules are lacking when it comes to ensuring consent to share personal data.

Many participants noted that there are insufficient standards and rules in place to ensure that consumers are only sharing the data they need to share to access services. An example provided by one participant: "When you go to the liquor store, they ask for your ID to prove you're of legal drinking age. When the cashier asks for your ID, usually a driver's licence, they not only have access to your age, but a myriad of other personal information." The issue of consent was also raised, and some participants noted that sharing personal information should be based on consent.

EXAMPLES OF CURRENT STANDARDS:

- The Pan-Canadian Trust Framework (PCTF)
- Open standards for APIs

Future State of Digital ID and Open Banking

In the second half of **breakout group discussions**, participants were asked to provide their views on the desired future state of digital ID and Open Banking in Canada.

Recurring themes and key insights from the discussions are summarized below.

Q2.1: What is the ideal future situation of digital ID and Open Banking in Canada (i.e., what are the ideal use cases, what benefits can consumers/service providers reap from increased use of digital identity)?

Theme #5: A paradigm shift to a consumer-centric model, where individual consumers own and control their data.

One of the most recurring themes from the discussions was the idea of a paradigm shift from institutional data ownership and control to a more transparent and democratic consumer-centric model. It was noted in multiple sessions that individual consumers should be empowered and equipped to control who has access to their personal data and how it is used and shared. Several questions were raised about this topic: "How can we give the user control? How can we let them leverage their own information and use it where they see fit?"

In one session, it was suggested that giving consumers access to their digital ID could create easier access to multiple bank accounts. The consumer could give permission to the institutions they want their data shared with, and they could revoke permission to institutions to share data between each other.

In discussing the shift to a consumer-centric model, participants noted that education will be key to making it a reality. Consumers will need to know how much control and power they have over their own data as well as the benefits and risks associated with digital ID and Open Banking. For example, one participant said that, as a consumer, they do not know where their data is going even though they pay attention to consent. "Even when you do pay for something, you still don't know where your data is being disclosed, which is troubling. This does not foster trust." This concept of "informed consent" was explored throughout the sessions, and participants noted that its definition needs to be clarified and made easier to understand.

Theme #6: Interoperability creates inclusion and value.

The benefits and value of interoperability was discussed in several sessions, specifically as it relates to access to data across systems, provincial jurisdictions and international borders. Several participants noted the consumer benefits that could be realized, citing examples of people living and working in different regions across Canada and other countries being able to have access to their digital ID and personal and financial data to access local services.

Participants explained that interoperability is not just about technology but also about the system of laws, regulations and international standards. Protocols and regulations need to allow for all entities to work together.

In addition, it was raised that broad participation is a prerequisite for interoperability to be realized. If major industry players sit on the sidelines or the barriers to participation are too great for small and niche service providers, the value and benefits for consumers will be limited.

Q2.2: What rules, regulations or standards are necessary for a digital identity and an open banking framework in Canada?

Theme #7: Focus on privacy.

Participants noted that strong privacy protections are needed to minimize the risk of personal information being overshared, mishandled or otherwise compromised. One participant suggested a decentralized system may be more resilient and secure, as a centralized system has a single point of failure and data is more vulnerable to attack/fraud because it is stored in one location.

Theme #8: Harmonization and creation of a National Digital ID Framework.

Participants noted that Canada needs a comprehensive digital ID system that works at both national and provincial levels and provides a clear, simple way to achieve a level of trust with the Canadian public.

Discussions highlighted that digital ID will be up to the provincial governments, so there is the challenge of jurisdiction for this. There needs to be harmonization across federal and provincial jurisdictions to ensure the system works seamlessly across the country.

Theme #9: Establish clear definitions and use consistent terminology.

Participants felt there is confusion among consumers about what digital identity actually is and how it impacts them. Digital identity needs to be clearly defined and articulated before considering how it impacts certain sectors such as banking. It was also noted that the differences between “digital ID” and “Open Banking” need to be made clearer. There was also discussion around the term “Open Banking,” with some participants suggesting it implied a “laissez-faire” or “wild west” system, so participants suggested the term “consumer-directed finance” be used instead. It was also emphasized that it is important to use plain language when trying to educate consumers, as jargon or more complex, technical vocabulary can cause confusion.

Theme #10: Learn from other countries and adopt international best practices.

As mentioned previously, participants recognize that other countries are more advanced in both digital ID and Open Banking. From a rules and standards perspective, participants saw this as an opportunity to learn from their experiences and adopt proven, successful approaches and best practices in Canada. These best practices can help inform the development of effective regulations and standards in Canada.

CONSIDERATION FOR FUTURE STANDARDS

Auditing: Certification and accreditation maintaining those standards where there is currently difference of interpretation.

- **Transactions:** Requirement for a standard way for transactions
- **Data sharing:** Create a technical framework and common standard for data sharing.
- **Standard around digital trust and identity:** Providing consensus-based requirements into the marketplace.
- **International cooperation among standard development:** For example, between Canada and the UK at the Open Data Institute (ODI).
- **Buy-in:** Standards need to encourage an operating model for people to come together and protect and promote businesses to buy in. Otherwise, standard adoption will take a long time.

Use Case Working Group Report

PREFACE

While there are frameworks and private-sector tools that Canadians can use for authentication, Canadians are lagging behind in having a recognized national digital identity or open banking system in place. This hinders Canadians from using online services and being able to safely share their data with whom they choose. Many Canadians rely on commonly used archaic authentication systems like physical ID cards, photos of physical ID cards, passwords and security questions that are time-consuming, not user-friendly, and at risk of forgery and fraud. Additionally, Canadians choose to either not share their data with innovative services for managing their finances or choose to share their data in a less secure manner.

The risks to Canada are threefold. First, there is the risk of Canadians not being able to benefit from a safer, more secure system of identifying themselves online and sharing their data. Second, there is the risk of technology advancing but without any formalized framework, which can diverge in many directions and prevent interoperability in the system. Third, there is a risk to Canadian innovators who are looking to grow their ideas in competition with innovators in other countries. Inaction means that Canada falls behind to foreign service providers and innovators.

It is imperative that Canada establishes a “people first, digital first” approach to empower privacy protection. Canada’s approach and design to solve digital identity is leading the world. The world is watching Canada because we are taking a public-private and people-partnership approach. We are focusing on economic benefits for all, while designing an approach with Canadians at the centre. This is unique about Canada and why so many countries are following our work. However, in terms of delivering actual digital identity to Canadians, we are behind. Canada urgently needs political will, innovative policy reform and technology standards-based adoption.

While digital identity and open banking are separate issues and can be discussed independently, this report combines discussion of both and their interdependence. This report supports the 35 recommendations of the Data Governance Standardization Collaborative Roadmap. The Roadmap lays out where Canada stands with regard to data governance and why standardization around data governance is essential. The Roadmap does not intend to instruct stakeholders on what to do but rather to inform them on the current standardization landscape for data governance and to effectively bring together fragmented conversations on complex and difficult issues. All recommendations are intended to help dissect relevant data governance issues and help close gaps, in support of the various government and industry initiatives that are currently taking place.

This report is based on a consensus of those who actively participated in its development and does not necessarily reflect the views of the individuals or organizations who participated in its development.

EXECUTIVE SUMMARY

The Data Governance Standardization Collaborative (DGSC) was established in the summer of 2019 as a cross-sector coordinating body with the objective of accelerating the development of industry-wide data governance standards and specifications that are consistent with stakeholder needs, and facilitating the growth of data governance capabilities in line with national and global priorities. The DGSC has more than 220 experts representing a broad range of stakeholders across all levels of government, Indigenous groups, academia, the private sector, NGOs, and privacy and ethics experts from around the country engaged in fulfilling its mandate. The DGSC is developing a roadmap for standards in good data governance, examining where standardization is required through several use cases.

With abstract concepts such as data governance and the role standardization can play in collection, sharing and use of data, it can be challenging to understand the impact or relate to it from an every day perspective, especially when data is an “intangible” asset. To help stakeholders understand the role standardization can have in supporting data governance and trust, use cases were used as relatable examples.

In the summer of 2020, the DGSC Use Case Working Group on Digital Identity and Open Banking was established with a small group of experts. The Working Group discussed the identified DGSC gaps as they relate to digital identify and open banking. The intent of the use case was not to design a standard or propose guidelines for digital identify and open banking but rather to clarify the gaps identified to support the DGSC roadmap, considering the following:

- Requirements for identity verification and authentication – with consideration for individuals who experience difficulties proving their identity or accessing online services;
- Consumer control of data, access and privacy;
- Security protocols for sharing client data (i.e., API standards);
- Operational guidelines for implementation and adoption risks; and,
- Client experience guidelines that reflect values of inclusion, transparency and trust.

Over a series of five meetings and a public consultation, members of the Working Group shared their perspectives on the challenges facing digital identity and open banking in Canada. The Working Group recommends taking immediate action, building on what has already been done, ensuring Canada does not fall even further behind.

Ultimately, seven principal recommendations emerged:

1. It is imperative that Canada immediately establish a “people first, digital first” approach to empower privacy protection, which is not the same as secrecy. It would benefit Canadians to have an established right to control their data and have the right to share their data with whom they choose. This requires a strategic, coordinated and multi-sector approach that will enshrine the rights of consumers to control and use their data. Canadians would benefit from government and industry working together to put in place regulatory frameworks as soon as possible, and consumers should be put at the centre of those digital identity and open banking frameworks.
2. A broad group of technical and policy practitioner expert stakeholders should collaborate to review and recommend adoption of the existing and emerging standardization and normative-type activities that take into consideration the needs and requirements of Canadians, building on existing work. This will require an assessment of the frameworks currently in place and analysis of whether current technological standardization efforts will meet those needs. Standards, such as National Standards of Canada, can bring together different points of view with standardization work that is consensus-driven and inclusive of industry, academia, consumers and government. Areas that would require standardization include:
    - Standards for accessing, storing, managing, transacting and sharing data;
    - Standards for privacy, security and transparency requirements;
    - Standards for interoperability across jurisdictions and industry verticals; and,
    - Standards for verified credentials, including clear levels of assurance to ensure interoperability.
3. Industry, academia, consumer groups and all levels of government (federal, provincial, territorial) should be active partners and participate in the development of National Standards of Canada, or other normative documents, and international standardization efforts. This includes collaboration and coordination with international standards bodies and taking an active role in promoting international adoption of any future Canadian standards where it makes sense to do so.
4. There is a need for strategic and tactical communication plans and investments in the education of consumers about their data rights and how they can express those rights. Digital identity and open banking are complex, and the engagement of Canadians is paramount to build knowledge and confidence around privacy and security issues.
5. Canadians need an overarching trust framework enabling people to access/share data safely. Any framework for digital identity and/or open banking should be in accordance with relevant national and international standards and best practices; legislation and oversight should allow for new innovations and use cases to emerge in the future. This could be the adoption/adaption/development of an existing/new framework, or through public-private collaboration. Government involvement is important, but any work should be done in collaboration with the private sector, as supported by 66% of Canadians.[35] This will ensure interoperability and address key issues such as privacy, security and cross-border interaction.
6. Standardization tools could be used to establish criteria for an accreditation framework that will allow for public and private organizations to issue and verify digital identities, and to receive and share data in an open banking system.
7. Public and private entities that collect and use personal data can set an example by making data into a useable and shareable form and by enhancing security protocols by moving beyond the use of passwords and security questions, which can be stolen or hacked.

This report focuses on the Digital Identity and Open Banking Use Case. For the purposes of this report only, the following definitions are being used as agreed by the use case working group (additional terms and definitions can be found at the end of this report):

[35] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.

Digital Identity (ID): Identity is a "collection of indicators (or attributes) about a person (entity) that make the person unique. Digital Identity (ID) is a set of attributes that links a personal entity with their online interactions by using trusted sources... [similar to] an online footprint." Digital ID also refers to the information used by computer systems to represent an external person or organization, allowing access to digital services safely, securely and efficiently. Digital ID provides consumers with more control of their data and identity by being able to choose what information to share on a need-to-know basis. It "can be standardized and used between entities, with the ability to add new information."[36]

Open Banking (Consumer-Directed Finance): Open Banking is a framework of regulations and standards that allows "consumers and businesses [to] authorize third party financial service providers to access their financial transaction data, using secure online channels."[37]

In the age of COVID-19, in-person interactions have become restricted, so operating in a digital context is becoming increasingly important for Canadians. Open banking (or Consumer-Directed Finance) is a prime example of this. Digital connectivity, data and consumer needs are driving institutions, governments and Canadians towards third-party arrangements. However, lack of regulation and standards to support this new sector, and tools to enable this such as digital ID, are leaving Canadians behind economically, competitively and, most importantly, with regard to security.

Various public-sector national initiatives have been established over the last two years in support of digital identity, open banking and the need for standardization. It is imperative that Canada build on what has already been done. For example, in 2018, Canada joined a network of countries looking to use digital technologies to benefit citizens. One element of this strategy is developing a trusted Digital ID platform.[38] Open Banking was also identified by the Senate Committee on Banking, Trade and Commerce as one of the key use cases that should be addressed by the Data Governance Standardization Collaborative (DGSC).[39] In 2019, the Department of Finance appointed an Advisory Committee to review the merits of Open Banking. Private-sector initiatives that include public-sector participants have also been moving forward, such as the work of the Digital ID & Authentication Council of Canada (DIACC) on the Pan-Canadian Trust Framework, the launch of the Canadian working group of the Financial Data Exchange (FDX) and the work of CIO Strategy Council on open banking standards, in collaboration with the Open Banking Initiative Canada (OBIC) and FDX. Most recently, the House of Commons Standing Committee on Finance published its February 2021 Committee Report, which made recommendations relevant to this work. Notably, Recommendation 128 calls for the implementation of a digital identity system that empowers Canadians to control their data held by the federal government, and Recommendation 129 calls for the creation of a national data strategy.[40]

According to DIACC, "consumers, businesses and government entities [must] work together to achieve the common goal of enabling a safe, secure and trusted ecosystem for Canadian digital identity."[41] Digital ID needs to be a top priority for policymakers, politicians and business leaders in order to bring digital ID policy into government, adjust language in the policy to accommodate for trusted digital ID and incentivize businesses to explore digital solutions in their organizations. Additionally, 83% of Canadians trust government to keep their data safe and 81% trust financial institutions.[42] Government and industry collaboration is essential, with 66% of Canadians wanting the public and private sectors to work together on a joint digital ID framework.[43] This is significant as it would allow federal, provincial and territorial governments to collaborate on the issuance of credentials, allow industry to play an active role in the development and usage of digital credentials, and allow for mutual recognition and interoperability between governments and private-sector

[36] DIACC. Industry Insights: Digital ID in Financial Services. https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.

[37] Department of Finance of Canada. A Review into the Merits of Open Banking. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html.

[38] Susan Crutchlow, TransUnion. Digital Identity – A Key Driver of Canada's Digital Economy. https://www.transunion.ca/blog/digital-identity.

[39] Senate of Canada. Report of the Standing Senate Committee on Banking, Trade and Commerce. Open Banking: What it means for you. https://www.sencanada.ca/en/info-page/parl-42-1/banc-open-banking/.

[40] House of Commons. Investing in Tomorrow: Canadian Priorities for Economic Growth and Recovery – Report of the Standing Committee on Finance. https://www.ourcommons.ca/DocumentViewer/en/43-2/FINA/report-1/page-21.

[41] DIACC. The Economic Impact of Digital Identity in Canada. https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.

[42] DIACC. Canadians are Ready to Embrace Digital Identity. https://diacc.ca/2019/10/15/canadians-are-ready-to-embrace-digital-identity-2/.

[43] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.

participants. Establishing standards would also ensure there is no misuse of client information and there are strict rules for privacy and security of client personal information and data.

Canadians want more control and agile access over their data, with 9 in 10 Canadians being supportive of digital ID, and a significant majority believe that it is important to the digital economy.[44] Millions of Canadians are already sharing banking information with third-party providers; however, due to a lack of a formal open banking regime, they are forced to rely on less secure methods such as sharing their online banking passwords with alternative financial service providers, putting their personal identity and sensitive financial information at risk. Having a formal digital ID system in place to fit in with the open banking regime would make authentication much easier for both consumers and service providers. Consumers would be able to share only the information required to authenticate them without having to use passwords that can be stolen. Service providers would be able to trust that a valid digital ID was used to access client information and not worry about clients having their passwords stolen. Alternative workarounds are a major security risk, as is the use of passwords and security questions that can be stolen. Not having digital ID and open banking is putting Canadians and their data at risk. With a Canadian digital ID framework, there are "**potential net savings per institution at or above CAD $100 million per year, through operational efficiencies... and reducing fraud.**"[45] With these challenges in mind, standardization can be a possible solution for implementing a Canadian digital ID framework, reflecting values that Canadians support (inclusion, transparency, trust).

Today, large technology companies have detailed knowledge of a person's likes and interests.[46] Financial institutions have knowledge of a person's interests and spending habits. Government departments and agencies know a person's biographical information. The only ones who cannot use the data are the people/businesses the data is about.

Digital authentication services are already being used in Canada. The most notable example is Verified.Me, by SecureKey, which is used by some government departments, healthcare providers, financial institutions and fintech companies (i.e., accessing Service Canada or CRA, filing taxes online, or banking online). Some provinces such as Alberta and British Columbia already have their own digital ID systems in place, while Ontario and Quebec have started moving forward with their own. However, in the absence of a Canadian identity management framework supported by robust standardization and regulation, there are challenges in the way that Digital ID works in Canada today. Online identities are fragmented across many businesses/entities, which increases the systemic risk of fraud through accumulating data. Data breaches occur and erode people's confidence in that organization and the digital economy.[47] Identity has traditionally been proven using physical records such as passports or ID cards. Unfortunately, physical documents can be forged or altered, and fraud accounts for significant financial losses. In addition, many Canadians do not have sufficient means to prove their identity, resulting in them being excluded from convenient digital access to services such as healthcare, government and banking. This has never been more apparent than during the age of COVID-19. A recent DIACC survey found that 75% of Canadians believe COVID-19 has made having a digital ID either "much more important" or "somewhat more important," while only 2% believe it is "much less important."[48]

The pandemic has restricted in-person interactions, so traditional sectors and institutions are having to react immediately to reshape their frameworks to adapt and compete in a digital environment. Government should also be able to take advantage of the digital ID and open banking system and use it for priorities such as CERB, NextGen HR and Pay, and pension system modernization, among many others. However, lack of regulation and standards for adaptive tools, such as digital ID, to enable this is leaving Canadians behind economically, competitively and, most importantly, with regard to security. According to a McKinsey study, on average, full digital ID could unlock economic value equivalent of 3% to 6% of GDP in 2030,[49] or about CAD $48-97 billion.

[44] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.

[45] DIACC. Industry Insights: Digital ID in Financial Services. https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.

[46] Jathan Sadowski, The Guardian. Companies are making money from our personal data – but at what cost? https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon

[47] DIACC. The Economic Impact of Digital Identity in Canada. https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.

[48] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.

[49] McKinsey Global Institute. Digital Identification: A Key to Inclusive Growth. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

Several countries are much further ahead with digital ID and open banking, while Canada is falling further behind. For example, Australia recently announced an investment of AUD $256.6 million (about CAD $243 million) in a digital ID system as part of an economic recovery plan in response to COVID-19.[50] Meanwhile, the European Union (EU) has introduced regulations on electronic identification and trust services (eIDAS), in which public-sector organizations in EU member states can accept each other's electronic identification (eID). The Netherlands has adopted eIDAS, which allows Dutch citizens "to use a national login key (like DigiD) to access public services in other EU member states,"[51] while citizens of other EU countries can use their own national digital ID system to access Dutch government services. While eIDAS distinguishes between different levels of assurance for identification, the Dutch government has also built a digital identity framework with a higher level of assurance.[52] The Dutch framework around digital ID includes 14 universal guiding principles, some of which include the right to a digital identity, establish use by natural persons and legal entities in public and private sectors, ensure privacy protection, ensure adherence to national and international standards, include flexible infrastructure and room for innovation, and ensure independent oversight. The Dutch government also clarified the government's role in relation to the digital ID infrastructure. The role of the Dutch government in its digital identity system is as legislator, policy creator, enforcer of repercussions, registrar, service provider (for government services), digital ID tool supporter and financier.[53]

Another example is Estonia, which is often considered the gold standard when it comes to digital ID and data rights. Estonian citizens and residents have access to their data and the ability to share it. Estonians have been able to use their government-issued digital ID to access various e-services digitally for more than 15 years.[54] Estonian electronic identity comes with a physical card. It is used for electronic identification, electronic signing and the secure transfer of sensitive data – and is effectively equal to face-to-face identification. The Estonian eID allows a citizen or permanent resident to securely use all government e-services as well as many private-sector e-services provided by businesses such as banks, telecoms, energy companies and many others. This means Estonians can use their eID for filing taxes (in three minutes for most people), voting, healthcare, prescriptions, schooling, land registry and business registry (in 15 minutes).[55] The eID card can also be used in grocery shops, bookstores, pharmacies, libraries, cinemas and so forth. Estonians can securely transfer confidential data through email or file-sharing platforms without the risk of compromising confidentiality and integrity. All this is done while being both time efficient and cost efficient. Estonia's eID is widely used, accepted and trusted by both the public and private sectors. It has made secure e-services a normal part of everyday life, saving time and costs for citizens, companies and the public sector.[56]

It is important to note that these countries are different from Canada, and their approaches may not be suitable in a Canadian context. However, they provide important policy learnings for Canada, such as the concept of digital identity being embedded in legislation to reassure public and private entities to accept digital identification, and to ensure that citizens, businesses and governments are able to use the digital identity system and digital information infrastructures. These international examples also serve as useful illustrations of where other countries stand and how far Canada is at risk of falling behind.

While 2019 brought the "Merits of Open Banking" consultation by the Department of Finance, in addition to the Canadian Digital Charter, Canadians are still behind in linking government identification with online credentials, which could be leveraged to promote enhanced security and customer experience. Given the nature of the sensitive information that could potentially be exchanged or stored, privacy and cyber security considerations should be a key priority for the government, industry and participating stakeholders.

[50] Prime Minister of Australia. Digital Business Plan to Drive Australia's Economic Recovery. https://www.pm.gov.au/media/digital-business-plan-drive-australias-economic-recovery.

[51] Government of the Netherlands. Everything you need to know about eIDAS. https://www.government.nl/topics/online-access-to-public-services-in-the-european-union-eidas/everything-you-need-to-know-about-eidas.

[52] Government of the Netherlands, Ministry of the Interior and Kingdom Relations. Digital Identity Vision: Building Trust in the Digital World. Presented by Dick Dekkers (Digidentity) to DIACC on Feb. 23, 2020.

[53] Government of the Netherlands, Ministry of the Interior and Kingdom Relations. Digital Identity Vision: Building Trust in the Digital World. Presented by Dick Dekkers (Digidentity) to DIACC on Feb. 23, 2020.

[54] E-Estonia. Watch how the eID makes life easier in Estonia. https://e-estonia.com/eid-in-estonia/.

[55] Startup Estonia. Why Estonia? https://startupestonia.ee/why-estonia.

[56] E-Estonia. Watch how the eID makes life easier in Estonia. https://e-estonia.com/eid-in-estonia/.

Open Banking does not have any formal structure in place in Canada. However, Canada already has an informal open banking system, where people are sharing information with third parties when they are not allowed to do so, leading to significant consumer protection, privacy and cybersecurity risks. For example, the Department of Finance estimates that almost four million Canadians are using third-party applications that access personal financial data, such as data aggregators that collect and store information to provide a single snapshot of a client's financial picture.[57] In order to do this, clients share their online banking login credentials with the third-party app, which is in violation of the terms and conditions set forth by the online banking platform and is also less secure. While privacy legislation does apply to third-party institutions for collecting, storing and managing the information they collect, consumers may lack guarantees or comprehension of how these requirements are followed (even if third parties clearly articulate how they maintain data security and privacy). Clients may not be aware of how to confirm third-party services are keeping their data safe, and if a data breach were to happen, clients also lack convenient mechanisms to file a complaint or obtain compensation. Despite this, almost 50% of Canadians are willing to share personal information with a financial institution in exchange for better products and services.[58]

Public- and private-sector actors acknowledge that data sharing between Canadians is already taking place and that it is being done at times in a manner that is not as secure as is facilitated through a true Open Banking environment. This is why it is essential for Canadians to have in place a structure for data sharing to take place in a safe way that will protect privacy and security. Once Canada has this data sharing and open banking framework, it can reap the benefits. Many Canadians are already looking to services that make it easier for them to understand and manage their finances. For example, Canadians want services for better financial product comparisons, personalized financial product offerings, aggregation of payroll/accounting information, and automation of cash flows and payments, among many others.[59] An open banking system will lead to more competition in the sector, resulting in better products and more efficient services, all within a structure that Canadians can trust to respect their data rights, consent and consumer protection, with proper regulatory oversight. Canadians who choose the use the system will be able to share personal financial data with institutions that have met the criteria to participate, giving them peace of mind that they can trust the institution with which they are sharing their information and that they have avenues for complaints and compensation should anything go wrong. While many Canadians will move entirely online for their financial services and stop going to bank branches, others will continue to use in-branch or telephone banking. Customers will have a better user experience being able to access banking services through the channel of their choice.

The Canadian Senate's report into open banking noted the economic benefits to Canada under open banking, "through increased growth and innovation in the fintech sector. If Canada misses this opportunity by failing to create a regulatory environment conducive to open banking, Canada risks falling behind."[60] Canadian financial institutions (banks, fintechs, etc.) face the risk of not being able to compete globally with financial institutions from other countries that operate in open banking systems. If Canada proceeds with an open banking system, Canadian companies will be able to compete internationally but also become leaders in the financial services industry.[61]

[57] Report of the Standing Senate Committee on Banking, Trade, and Commerce. Open Banking: What it means for you. https://www.sencanada.ca/en/info-page/parl-42-1/banc-open-banking/.

[58] Robert Vokes and Andrew McFarlane, Globe & Mail. Canadian banks need to prepare for open banking now or risk being left behind. https://www.theglobeandmail.com/business/commentary/article-canadian-banks-need-to-prepare-for-open-banking-now-or-risk-being-left/.

[59] Department of Finance of Canada. A Review into the Merits of Open Banking. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html.

[60] Senate of Canada. Report of the Standing Senate Committee on Banking, Trade, and Commerce. Open Banking: What it means for you. https://www.sencanada.ca/en/info-page/parl-42-1/banc-open-banking/.

[61] Department of Finance of Canada. A Review into the Merits of Open Banking. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html.

With regard to the formal standardization system, none of the large international standards bodies have published standards that are specific to open banking. Accredited SDOs in Canada, such as CIO Strategy Council, have commenced the development of a series of standards on open banking (CAN/CIOSC 110-x). Additionally, FDX, an American industry association that expanded into Canada, has published a standard for the use of APIs,[62] with more than 12 million consumers accessing their financial data through the standard.[63] With no formal open banking framework in Canada, it will be important to look internationally for examples of the work that has been done and the approaches taken by the countries that have implemented their own open banking systems. It is best to look toward the UK Open Banking Initiative (OBIE), the European Payment Services Directive (PSD2), the Singapore Financial Data Exchange (SGFinDex) and Australia's Consumer Data Right Act in order to analyze the approaches taken by other countries and pull out best practices that could be applied to Canada. This could include taking a sandbox approach as other jurisdictions have done. For example, OBIE launched a sandbox for developers to connect their apps to the APIs, allowing them to test apps and build an understanding of open banking tools, standards and security requirements.[64]

It is important to note that there is important work being done in standardization around digital identity, digital credentials and digital trust. This includes Canadian standards development organizations (SDOs), international SDOs, and publications/guidance written by consortia and industry associations. In Canada, CSA Group and CIO Strategy Council have both worked on standards related digital trust and identity, while internationally, ISO, IEC, ITU-T, IEEE, ETSI, NIST and W3C have published many standards on topics and technologies related to digital credentials but none for digital identity or open banking specifically (an overview of some of the relevant standards and organizations is included at the end of this report, while acronyms and description of these organizations are included in Annex F of Roadmap).

In support of international standardization work taking place within these various standards bodies, Canadian voices need to be at the table promoting Canadian innovation and IP. Government and industry participation in standards development ensures Canadian companies can expand their market opportunities and generate revenue domestically and globally.

Unfortunately, while there are advances in the use of innovative technologies, such as blockchain and AI, some services still require Canadians to rely on manual/analog systems that are time consuming and frustrating to use, or that use digital services that sacrifice security for expediency, such as some ID verification and account systems. COVID-19 has only made it more obvious that fully digital and remote solutions are critical for Canadians. For example, until recent changes were made by FINTRAC to allow for complete remote account opening, some banks allowed clients to open bank accounts online, but then required those clients to come in for an appointment with a banking representative in order to verify their ID in person before the account was activated. While financial institutions are moving toward a complete online experience, some online services still require clients to provide photos of physical pieces of ID, which are at risk of forgery, when completing a fully remote account opening. Additionally, clients who want to transfer their investment accounts from one financial institution to another have to rely on some institutions using manual processing and outdated tools (such as mail or fax machines) in order for those transfers to be completed. Should the mail get lost, or if the results are faxed to the wrong number, that client's private financial information can end up in the wrong hands.

When it comes to data rights and consumer control of data and the technological advancements that accompany it, countries such as Estonia, the Netherlands and Singapore, among others, have built the equivalent of a bullet train. Meanwhile, Canada is on a bicycle. As more time passes, the gap between the bullet train and the bicycle grows larger. It is imperative that Canadians get on a bullet train of their own; otherwise Canada runs the risk of never being able to catch up.

[62] Financial Data Exchange. Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5. https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_Open_Finance_Standards_And_FDX_API_4.5.aspx.

[63] Newswire. Financial Data Exchange Adds 39 New Members with Expanding International Footprint. https://www.newswire.ca/news-releases/financial-data-exchange-adds-39-new-members-with-expanding-international-footprint-838469346.html.

[64] UK Open Banking Initiative. Developer Zone: Do you have test environments for TPPs including a sandbox? https://openbanking.atlassian.net/wiki/spaces/DZ/pages/22872552/Do+you+have+test+environments+for+TPPs+including+a+sandbox.

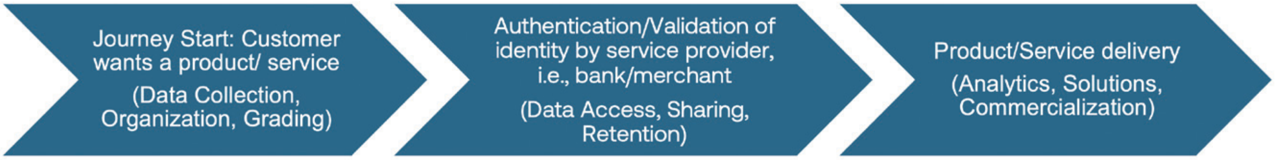
USER STORIES

Based on the extensive experience of the Working Group, a survey was circulated to capture members' current experiences along the Digital Identity and/or Open Banking lifecycle, either from a personal perspective or an organizational one. In addition to survey questions, members were also asked, from their perspective, to consider:

- what is the **risk of inaction** for Canada in NOT having a digital identity framework or an open banking framework?
- In an ideal world, **what micro-level actions are needed to move forward**?

Members were meant to answer the questions in light of the lifecycle assessment diagram below – what currently takes place within a user story – and what is the desired future that will bring value to Canadians.

Lifecycle Assessment of Digital Identity & Open Banking Use Case:


Journey Start: Customer wants a product/ service
(Data Collection, Organization, Grading)
Authentication/Validation of identity by service provider, i.e., bank/merchant
(Data Access, Sharing, Retention)
Product/Service delivery
(Analytics, Solutions, Commercialization)

Digital ID and Open Banking Use Case members were asked to provide their insight into their personal or organizational experience with a data journey as it relates to digital identity, open banking and standardization, and how it incorporates values such as inclusion, transparency and trust that are important to Canadians. A significant challenge the group identified was the lack of understanding of how digital identity and open banking are applicable to the lives of everyday Canadians. These are a few stories that can illustrate the concepts and the stories shared by the experts in the Working Group.

DEALING WITH THE AFTERMATH OF THE DEATH OF A LOVED ONE

A widow has to deal with the complex process and endless tasks of settling her husband's estate after his passing. This includes being established legally as the executor of the estate and having to do it with every single institution separately (governments, financial institutions, etc.). The estate process today is difficult, complicated and emotionally draining for anyone, but especially for someone who suffered a serious loss.

The estate process could be made significantly easier through trusted online verification (rather than in-person, by mail, or over the phone), and the possibility of data sharing between trusted institutions. This would mean an executor would only have to show ID once to get verification and, moving forward, would be able to take care of everything with all financial institutions and levels of government. This would allow for a significant unburdening for people to accomplish tasks as executors or powers of attorney, including the significant reduction in the physical and emotional toll taken by the current process.

PAYING RENT

A landlord collects payments from a tenant. The current process is not complicated for either party, as usually the tenant will provide a void cheque to the landlord, who will take it to the bank. The challenge here is the amount of personal information that the tenant must share, namely his/her bank account number. The tenant has no control over how that information is used or stored once he/she hands their void cheque to the landlord.

Tenants will have more control over what and how their data is shared and stored, and pre-authorized payments can be done without sharing more information than is necessary.

ACCESSING PERSONAL FINANCIAL DATA FOR SECONDARY USES

Consumers should have access to their personal and transactional financial data and be able to access it for various purposes. However, there are security risks to this, such as fraudulent uses of devices, phishing attacks and identity theft.

Consumer control over their own data would allow them to access various services that will help with improved decision making, and improve information security and competition in the marketplace. Connections can also be made to digital ID as a potential solution to the security risks in our current reality.

MANAGING PERSONAL OR BUSINESS FINANCES MORE EFFECTIVELY

From an individual's perspective, there can be a desire to manage personal finances more easily through connecting all accounts and assets into one user-friendly platform.

From a business perspective, a manufacturing co-op, for example, managing administrative work and finances could do so much more securely with digital ID and open banking.

Digital ID could allow institutions to trust that only the authorized people to make decisions are the ones doing so. In terms of open banking, it will allow individual users, businesses or governments to share data how they choose, in ways that are more secure and more efficient that current methods.

The common theme throughout these user stories centres around current difficulties associated with sharing data, accessing data, or data storage in a single location. In the case of the landlord and tenant, the problem is the opposite: the tenant must share too much data and is not sure how the landlord will store that data.

The lack of digital ID and open banking frameworks prevents Canadians from completing tasks more effectively and efficiently, meaning they must either rely on dated analog technologies or, if they choose to do things more efficiently, compromise their security by sharing online passwords or sending images of their personal information through less secure methods. In addition to an economic toll, there is also a significant emotional toll. In situations where Canadians must deal with inefficient and tedious administrative processes, there is significant frustration from users who are used to having things done online and in a quicker amount of time.

Digital ID will allow for the creation of trust through the authentication of an individual, or of individuals that are part of an organization, for faster, safer and more efficient data sharing processes to take place. Open banking will allow consumers to have better control over their information and to share and use their financial data more effectively. This will improve decision making and security and help foster competition in the marketplace. Both will help eliminate legacy infrastructure that is not user friendly in favour of new technological advancements.

RESULTS OF SURVEY

Survey respondents looked at each of their use stories and then broke them down into four broad areas.

1. Foundations of Data Governance for Open Banking and Digital Identity

Survey participants were asked to explore the current practices when a person begins to use a product/service, i.e., opening an account or starting a transaction. For example, how much assurance do organizations have that the customer is who they say they are, or do customers have that the service provider is who they say they are? Does current regulation allow the use Digital ID for this transaction? As a customer, how much do you trust the organization with your data, and why do you trust or not trust them? As a service provider, what security is in place for customers that you know of? As a customer, do you know if your data is being used for secondary purposes? As a service provider, do you have secondary uses for the data and, if so, what are they? Do customers know this?

Respondents were also asked about the desired future. For example, what macro-level actions are needed to reap positive benefits from digital ID and open banking? What value will be created for Canadians? What role can standardization and/or regulation take in this? What can be done to ensure interoperability is fundamental?

With regard to the foundations of data governance and the current situation, participants identified that it is difficult to obtain or share necessary data and that digital ID cannot be used in most cases. Physical pieces of identification are still the most used methods of verifying ID, but they also can be forged. Due to the lack of a digital ID system, some tasks cannot be completed online, while others are too reliant on and place too much trust in passwords. This can be incredibly burdensome and challenging for many administrative processes that could be completed much more simply online.

Experts also identified the key issue of poor data security. There is trust in certain institutions when it comes to data security due to their reputations (i.e., government, financial institutions, healthcare providers). Regulations are in place around data protection that prevent sharing with third parties; unfortunately, there are many other instances where organizations may not have followed the privacy or data protection controls, or those controls may have been breached. Aside from this, trust in some organizations is low, especially due to deliberately complex user agreements, and stories of fraud and misuse of data in the headlines.

Another key issue is the lack of control over one's data. Many service providers use and analyze consumer data to create value for both the service provider and the consumer. Consumers are usually aware (assuming they read the terms of service) but do not have the ability to request anonymity or block advertising related to the data, or the ability to share that data.

Participants are supportive of the adoption of digital ID and open banking in the future, ensuring secure online methods of accessing and managing data would exist. Both would create great value to Canadians by making many processes easier, saving time and reducing costs, among other benefits. Support and adoption by all levels of government and major private-sector institutions would enable widespread adoption to move away from archaic processes (e.g., faxes, paper documents). Standards would help ensure privacy, security and interoperability between new systems and with legacy systems, and allow new innovations to thrive. Standards for data classification, sharing, handling and storing could help ensure there is consistent implementation and inclusion of service providers while remaining technology agnostic.

2. Starting an Online Activity (Data Collection, Organization, Grading)

Respondents were asked to describe, from their perspective and experience, what type of information is required to establish identity. Questions included how this information is collected and where it is stored. Are their concerns around the quality of the data collected and the status of documentation framework (standards, best practices, certifications) used.

Questions on the desired future asked respondents, from their perspective and experience, what type of information should be requested to establish identity and how Digital ID would support this.

Currently, physical documents are generally required to establish identity, which often includes some in-person activity at some point in the process. Multiple forms of ID are often required, and most of these processes are inefficient. Electronic copies of physical documents may be used in some places, but they may not be sent securely. Sometimes clients may send documents through email, which is only secure if done by using encrypted email (which most Canadians do not know how to do). There have been advances in authentication technology (PINs, two-factor authentication, biometric authentication, etc.).

In the desired future, digital ID and open banking would allow for easy, secure distribution of data for various purposes and full consumer control of their data to manage life events, finances, etc. In particular, this would enable only the specific information necessary to be shared, and not too much. There would be government and industry involvement in the system, as well as appropriate oversight of the system. A strong education campaign would be necessary to teach Canadians about their rights and how to use digital ID and open banking, as only about half of Canadians are at least somewhat familiar with digital ID.[65] Citizens would be able to easily aggregate their data and make better financial decisions, while businesses would benefit from lower resource requirements, easier verification of suppliers and less fraud.

3. Public API, Bank Data, Bank Apps – Where does the data go? (Data Access, Sharing, Retention)

Questions around current practice asked respondents to identify who can have access to customer data (internally, externally), if this data is shared with third parties and what standards or certification practices are used for this. What does the desired future look like?

Many institutions have strict rules with regard to the handling of customer data, ensuring that only authorized personnel have access. Financial institutions do not share personally identifiable information (PII) with third parties; any information shared with a third party for a value-add is masked or anonymized, due to strict requirements within privacy legislation, such as PIPEDA (organizations in other industries in Canada are also required to follow the same privacy legislation).

Additionally, ISO 20022 is a common standard for data exchange and payments messaging followed by the financial industry, although it does not contain security requirements within the standard. In other industries, however, data handling may not have the same strict rules, especially when processes are manual.

[65] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.

More than three-quarters of consumers are comfortable with data being shared with a third party when they receive something in return (e.g., lower costs, better service).[66] Consumers do have high expectations in return, expecting full control of their data, the ability to opt-out and full transparency over who has access to their data, for what purpose, and what security measures are in place to ensure data is not retained or exposed. Some of the stories shared include support for consumers having the ability to review and monitor who has accessed their data and compare service providers based on their services and security measures in place, which would be enabled by standards. Some of the survey respondents are also in favour of requiring minimum standards for institutions to participate in the system and establishing a recognized conformity assessment program.

4. Product / Services (Data Analytics, Solutions, Commercialization)

The last questions for respondents focused on what third-party providers can do with the data they have access to (what kinds of analytics, with whom are they allowed to share the results of those analytics, etc.). What is the desired future state? For example, what regulations or standards would help Canadian businesses grow and what would hinder businesses or their ability to deliver a product or service? What value is created to benefit Canadian consumers and service providers?

Data analytics has many uses and benefits for consumers and service providers, such as removing frictions in various processes and improving decision-making abilities. Digital ID can simplify consent management processes, for example. For open banking, regulation will determine the scope of data, what data enhancement is possible and how it will be shared.

The desire for the future is to make services faster, easier, less expensive and more efficient and transparent – whether with payments, estate settlement or other examples. Through education, consumers with more control of their data will be empowered to be more aware and involved with the value of their data. Consumers will also be more aware of the revenue models of the services they use. Parents, legal guardians and caregivers see digital ID as an important tool to help manage care for their children or ageing parents, for tracking health records/immunizations, signing consent forms, registering/managing government programs, or acting as legal representatives or powers of attorney.[67]

Ideally, adoption of digital ID can deliver important societal benefits, especially by making an open banking framework operate better by minimizing the risks and inefficiencies of current systems and processes. Standards can play an important role in ensuring that all these goals can be achieved, in particular as a way to avoid overly prescriptive regulations that would stifle innovation.

PUBLIC CONSULTATION FINDINGS

In December 2020, SCC and the DGSC hosted a series of dialogue sessions with Canadians on the topics of digital ID and Open Banking. Two of the sessions were held in English, while the third was held in French. The sessions were attended by more than 100 participants from across the country, including representatives from financial institutions and third-party service providers. Each session began with a brief presentation by SCC officials on the role of the DGSC, the importance of standards, and the current state of digital identity and open banking in Canada. Participants were then invited to contribute to a conversation focused around two main areas of discussion, namely:

- the current situation of digital ID and open banking in Canada, including existing challenges, opportunities, rules and standards; and,
- the ideal future state, from the desired benefits for consumers to the laws and regulations needed for effective digital ID and open banking frameworks.

[66] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.
[67] DIACC. Canadian Digital Identity Research 2020. https://diacc.ca/2021/02/16/covid-has-accelerated-canadians-demand-for-digital-id/.

CURRENT STATE AND CHALLENGES

During an interactive whiteboard activity at the outset of the discussions, participants shared their perspectives on the challenges facing digital ID and open banking in Canada. Ultimately, four recurring and overarching challenges emerged:

1. Trust, and the need to earn and maintain the confidence of consumers;
2. Security, and the need to manage risk, protect privacy and prevent fraud;
3. Fragmentation, and the need to optimize cooperation, interoperability and efficiency; and,
4. Effective governance and oversight, and the need for consistent rules, regulations and standards that are aligned across jurisdictions

Following the whiteboard exercise, participants engaged in small breakout group discussions. When reflecting on the current state of digital ID and open banking, participants generally felt that Canada is extremely well-positioned to become a front-runner in both areas; however, there was also agreement that we are falling behind other countries in developing the necessary legal and regulatory frameworks. Multiple participants noted that more leadership and support is needed from the Federal Government as there are currently no laws to enable and govern open banking in Canada. Consumer awareness and education was another gap identified by participants, who said Canadians lack the understanding needed to use and trust digital ID and open banking systems. However, it was also noted that there is a shared onus on governments and industry to ensure that individuals are aware and confident in open banking.

IDEAL FUTURE STATE

When looking ahead to the desired future state of digital ID and open banking, participants generally agreed that the individual consumer should have greater control and decision-making power when it comes to who has access to their personal data and how it is used. This, participants felt, would require a fundamental paradigm shift from institutional data control to a more transparent and democratic consumer-centric model – i.e., decision-making power, customer-centricity, interoperability and adoption. Participants envisioned a comprehensive and trustworthy national digital ID system that works seamlessly across national and provincial levels, and they underscored that broad participation and interoperability together with strong privacy protections are critical to success.

RECOMMENDATIONS

Supporting the seven principal recommendations outlined in the Executive Summary, the commonly held view among consultation participants and Use Case experts is that Canada can be a global leader in new technology associated with digital ID and open banking but is falling behind other countries due to the lack of development of the necessary legal and regulatory frameworks. It is imperative that Canada start taking incremental steps to move forward as soon as possible in solving the main pain points and inefficiencies, rather than waiting for perfection.

The main problem is the current approach taken by Canadian laws regarding privacy, which are designed to look at the concept of data through a narrow lens, for example, the focus on data protection and privacy, as opposed to data sharing. Regulation may not be providing enough focus on consumer control of data and consumer choice of who has access to the data about them, in a way that is transparent and incorporates consumer control in combination with data privacy and protection. This idea is not a zero-sum game; data protection and data sharing go hand-in-hand to empower privacy, according to privacy-by-design.

The shift in perspective that Canada needs to embrace is that Canadians must have greater control of their data. As a result, Canadians must be entitled to control their data, including who has access to it. It does not erode privacy rights or data protection; it strengthens and enables privacy and data protection by putting it in the hands of Canadians themselves to control and use for their own purpose for what they define as important.

With regard to next steps, it is imperative that Canada move as soon as possible, building on what has already been done and ensuring engagement of a broad spectrum of Canadian citizens and businesses. The longer Canadians must wait for digital ID and open banking, the further Canada falls behind with the risk of never being able to catch up.

The concern from many participants is the risk of inaction. Canada needs to take a proactive approach as soon as possible for the economic and security benefits, but also to avoid or mitigate the risks of inaction (falling behind other countries, being vulnerable to breaches).

Several participants have shared their view that Canada is already operating in an open banking environment, with people sharing personal information such as their online banking passwords in order for new service offerings to be able to access their data. However, there are no frameworks in place to ensure consumer and data protection and interoperability.

Meanwhile, not having a digital ID system in place prevents Canadians from safely and securely using online services and means they must rely on the archaic authentication system in place (physical ID cards, photos of ID, passwords, security questions) that is time-consuming, not user-friendly and which is at risk of forgery and fraud.

The risks to Canada are threefold. First, there is the risk of Canadians not being able to benefit from a safer, more secure system of identifying themselves online and sharing their data. Second, there is the risk of technology advancing but without any formalized framework, which can diverge in many directions and prevent interoperability in the system. Third, there is the risk to the Canadian innovators who are looking to grow their ideas in competition with innovators in other countries. Inaction means Canada falls behind to foreign service providers and innovators.

Many Use Case experts view the role of public- and private-sector collaboration as significant in moving this work forward. Formal adoption through standardization of the necessary frameworks for enabling digital ID and open banking is seen as the most effective way to move Canada forward in a quick and efficient way – for us to have a safer Canada.

KEY TERMS

For the purpose of this document, below is a list of key terms and nomenclature to facilitate the understanding of the user journeys described.

Authentication
Authentication is the “process of establishing truth or genuineness to generate an assurance of credential or identity.”[68]

Consent
Consent indicates that an authorized used has given permission “to share Identity and/or Personal Information about a Subject as per the terms defined in a Notice.”[69]

[68] DIACC. Proof of Concept – Online Proof of Residency. https://diacc.ca/wp-content/uploads/2016/06/Online-Proof-of-Residency-POC-FINAL.pdf.

[69] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

Digital Identity (ID)
Identity is a "collection of indicators (or attributes) about a person (entity) that make the person unique. Digital Identity (ID) is a set of attributes that links a personal entity with their online interactions by using trusted sources… [similar to] an online footprint."

Digital ID also refers to the information used by computer systems to represent an external person or organization, allowing access to digital services safely, securely and efficiently.

Digital ID provides consumers with more control of their data and identity by being able to choose what information to share on a need-to-know basis. It "can be standardized and used between entities, with the ability to add new information."[70]

Entity
An entity is something "with a distinct and independent existence, such as a Person, Organization, or device, that can be Subject to legislation, policy, or regulations with a context, and which may have certain rights, duties, and obligations."[71]

Identity
Identity refers to "physical or digital information about a Subject that uniquely identifies a Subject within a context, and is used exclusively by that same Subject, or by a Person acting on behalf of an Organization, to access online services with trust and confidence."[72]

Open Banking (Consumer-Directed Finance)
Open Banking is a framework of regulations and standards that allows "consumers and businesses [to] authorize third party financial service providers to access their financial transaction data, using secure online channels."[73]

Organization
An organization is a legal entity "that consists of a person or organized body of people with a similar purpose, and whose existence is established by legal statute."[74]

Person
A person is "a biological individual, human being who is alive or deceased."[75] This includes "minors and others who might not be deemed to be Persons under the law."[76]

Personal Information
Personal information includes any "factual of subjective information, recorded or not, about an identifiable individual" or person.[77]

Service
A service is a "valuable action, deed, or effort performed to satisfy a need or to fulfill a demand."[78]

Standardization
Standardization is the development and application of standards publications that establish accepted practices, technical requirements and terminologies for products, services and systems.

Standards help to ensure better, safer and more-efficient methods and products, and are an essential element of technology, innovation and trade.

[70] DIACC. Industry Insights: Digital ID in Financial Services. https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.

[71] CIO Strategy Council. Digital Trust and Identity – Part 1: Fundamentals. https://ciostrategycouncil.com/standards/implement-standards/.

[72] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

[73] Department of Finance of Canada. A Review into the Merits of Open Banking. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking.html.

[74] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

[75] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

[76] CIO Strategy Council. Digital Trust and Identity – Part 1: Fundamentals. https://ciostrategycouncil.com/standards/implement-standards/.

[77] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

[78] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

Validation
Validation is a “process that confirms the accuracy of digital identity information about a Subject as established by an Authoritative Party.”[79]

Verification
Verification is the “process that confirms that the digital identity information being presented relates to the Subject who is making the assertion.”[80]

CURRENT STANDARDIZATION INITIATIVES

With regard to standardization initiatives, there is a lot of important work being done around digital identity, digital credentials and digital trust by Canadian SDOs, international SDOs, and industry consortia and associations. Please note this is intended to provide an idea of existing work and is not an exhaustive list.

Most notably, W3C has standards called the Verified Credentials Data Model and Web Authentication: An API for accessing Public Key Credentials Level 1, and also has two currently in development called Credential Management Level 1 and Web Authentication: An API for accessing Public Key Credentials Level 2. W3C has working groups that are specifically addressing standards in identity, credentials and authentication, though their standards catalogue is smaller than that of NIST and ITU-T. NIST has published guidelines on digital identity, including:

- Digital Identity Guidelines (NIST SP 800-63-3);
- Digital Identity Guidelines: Enrollment and Identity Proofing (NIST SP 800-63A);
- Digital Identity Guidelines: Authentication and Lifecycle Management (NIST SP 800-63B); and,
- Digital Identity Guidelines: Federation and Assertions (NIST SP 800-63C).

Meanwhile ITU-T has published frameworks that define principles around digital identity, including:

- Policy Framework including Principles for Digital Identity Infrastructure (ITU-T D.1140);
- A Framework for User Control of Digital Identity (ITU-T X.1251); and,
- Universal Authentication Framework (ITU-T X.1277).

There are numerous standardization organizations involved broadly in the IT and information management space. IEC, ISO, ITU-T, IEEE, CEN/CENELEC, ETSI, NIST, IETF and W3C all have published multiple standards around this subject. ISO has published numerous standards in IT, security, blockchain, information security management, and authentication; however, none are specific to digital credentials or digital identity. IEEE has published standards related to cryptography, encryption and blockchain and has many standards currently under development for those topics, including age-appropriate digital services, data management and open data – most notably the Standard for Blockchain-based Digital Identity System Framework. In Europe, CEN has published standards on ID card systems, while ETSI has standards on e-signatures, smart cards, cryptography, identity management and access management. Consortia have published complementary protocols and standards, such as IETF’s standards for Internet protocols OAuth, JSON and SAML, among others.

These entities each have a variety of technical committees developing the identified standards. For example, ISO, ITU-T and ETSI all have technical committees that work on topics related to digital credentials but none that specifically focuses on credentials or identity. CEN’s technical committee on personal identification and related personal devices (CEN/TC 224) might be among the most relevant to monitor, given its technological scope and strategic alignments.

[79] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.
[80] DIACC. Pan-Canadian Trust Framework Glossary. https://diacc.ca/trust-framework/pctf-glossary/.

At the national level, SCC accredits 12 SDOs that must follow a stringent standards development process, which includes a balanced group of stakeholders (industry, academia, government, consumer groups), and works on developing standards by consensus. Two of the 12 SDOs – Canadian Standards Association (CSA) Group and CIO Strategy Council – have published standards that are relevant to this subject matter but as of yet none specifically on digital credentials (although work is underway, as described below). CSA Group has adopted a significant number of ISO standards in the IT, IT security and cybersecurity space and published them for use in the Canadian market. It should also be noted that CSA work is referenced in the Personal Information Protection and Electronic Documents Act (PIPEDA) and may be referenced in future iterations of privacy legislation that replace PIPEDA. Although none are specific to digital credentials, they do include areas such as identification cards, entity authentication, cryptography and information protection, among others. Some notable standards include:

- IT Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques (ISO/IEC 9798-3);
- IT – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms (ISO/IEC 14888-2);
- IT – Security techniques – Encryption algorithms – Part 5: Identity-based ciphers (ISO/IEC 18033-5);
- IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts (ISO/IEC 24760-1); and,
- IT – Security techniques – Identity proofing (ISO/IEC TS 29003).

CIO Strategy Council has published foundational standards in data governance and digital trust and identity, including CAN/CIOSC 100-2:2020: Data governance – Part 2: Third-party access to data, which offers guidelines to ensure safety of information shared in remote, third-party interactions. One standard under development is CAN/CIOSC 100-7: Data governance – Part 7: Operating model for responsible data stewardship, providing minimum requirements for fiduciary stewardship, accountability and management in the collection and exchange of data. It is also currently working on standards directly relevant to digital credentials – Digital trust and identity – Part 3: Digital credentials (CAN/CIOSC 103-3) – and digital wallets – Digital trust and identity – Part 4: Digital wallets (CAN/CIOSC 103-4). These are part of a series of standards on digital identity and trust, the first of which (CAN/CIOSC 103-1) has been published while the remaining three are under development. One of its technical committees is dedicated to Digital Trust and Identity, which is currently working on these standards. As an SCC-accredited SDO, CIO Strategy Council has published four National Standards of Canada (NSCs).

Outside the traditional voluntary standardization system, there are many organizations involved in the digital credential or digital identity space that have also published various standards, technical reports, guidance documents or similar publications. For example, the W3C Working Draft on Decentralized Identifiers (DIDs) v1.0 is available on GitHub for parties interested in joining the discussion and development, after creating an account on the platform. Other organizations bring together significant industry players and advocate for the advancement of digital identity, digital credentials, or related technologies. In Canada, the Pan-Canadian Trust Framework (PCTF) promotes private-public collaboration in safeguarding digital identities online through a framework with standardized processes and practices across the ecosystem and builds trust in digital services in allowing modernized digital service delivery.[81] The PCTF is a suite of auditable normative-type documents that have been developed through a collaborative approach between the Digital ID and Authentication Council of Canada (DIACC), a non-profit neutral forum, and the Pan-Canadian Identity Management Sub-Committee of the Joint Councils of Canada, a forum consisting of the Public Sector Chief Information Officer Council and the Public Sector Service Delivery Council.

[81] DIACC. The Pan-Canadian Trust Framework. https://diacc.ca/2016/08/11/pctf-overview/.

Another example includes the work of the OpenID Foundation, which is a non-profit that serves as a public trust organization representing the community of developers, vendors and users of identity technology. Its work includes several specifications under development within its Financial-grade API (FAPI) Working Group, such as an API security profile.[82]

The Kantara Initiative is incorporated in the United States and the EU and has developed an Open Consent Receipt industry standard.[83] The initiative has also collaborated internationally with ISO, where Kantara has a liaison with ISO/IEC JTC 1/SC 27 on Information Security, Cybersecurity and Privacy Protection. There is also the Decentralized Identity Foundation (DIF), which is an industry group with global participation that promotes the enablement of decentralized identity solutions so that entities gain control over their identities and trusted interactions can occur. The foundation supports industry-wide discussions, contributes to open-source code and supports interoperability.

Additionally, the FIDO Alliance, the Internet Society, Hyperledger and OASIS have also published relevant consortia standards. Since these organizations are not accredited SDOs, their publications may not be recognized within the formal standardization system, unless the organization has specifically reached out to an accredited SDO and requested collaboration. This is the case for OASIS, for example, which participates in global standards development at ISO through the American standardization body, ANSI. It is currently active in ISO/PC 317 Privacy by Design for Consumer Goods and Services, and ISO/TC 324 Sharing Economy. Although SCC does not have an empirical approach to measuring the adoption rates of these associations' publications, these organizations can have significant memberships, both in terms of membership size and influence, that can indicate the extent of their industry reach and impact. Several multinational firms are members of one or more of these organizations, including Amazon, Apple, Bank of America, Facebook, Google, Microsoft, Visa, Nokia, IBM, Cisco, Dell, Huawei, Red Hat, TELUS and Walmart, among many others.[84,85,86,87]

As for open banking, none of the large standards development organizations has published standards. However, an industry group, Financial Data Exchange (FDX), which recently expanded into Canada from the US, published a standard for the use of APIs for consumer data sharing in an open finance system.[88] FDX and the Open Banking Initiative Canada (OBIC) both partnered with an SCC-accredited standards development organization, CIO Strategy Council. Through this partnership, CIOSC launched work in 2020 on developing a series of national standards on open banking (CAN/CIOSC 110-x).[89]

Additionally, it will be important to look at the work being done internationally by countries that already have open banking systems in place, including the UK Open Banking Initiative (OBIE), the European Payment Services Directive (PSD2), the Singapore Financial Data Exchange (SGFinDex) and Australia's Consumer Data Right Act, in order to analyze the approaches taken by other countries and pull out best practices that could be applied to Canada.

[82] OpenID Foundation. What is the Financial-grade API (FAPI) WG? https://openid.net/wg/fapi/.

[83] Kantara Initiative. Kantara Initiative Releases the First Open, Global Consent Receipt Specification; Meets GDPR Requirements, Free For Download. https://kantarainitiative.org/kantara-initiative-releases-first-open-global-consent-receipt-specification/.

[84] FIDO Alliance. FIDO Members. https://fidoalliance.org/members/.

[85] Internet Society. Our Organization Members. https://www.internetsociety.org/about-internet-society/organization-members/list/.

[86] Hyperledger. Members. https://www.hyperledger.org/about/members.

[87] OASIS Open. Members. https://www.oasis-open.org/member-roster/.

[88] Financial Data Exchange. Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5. https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_Open_Finance_Standards_And_FDX_API_4.5.aspx.

[89] Financial Post. CIO Strategy Council Advances National Standards for Consumer Directed Finance. https://financialpost.com/globe-newswire/cio-strategy-council-advances-national-standards-for-consumer-directed-finance.

More broadly, while international standards bodies may not have published open banking standards, they have published various standards that are specific to the financial sector and security that would be important for consideration within an open banking framework. For example, ISO has a technical committee on Financial Services (ISO/TC 68) that has published:

- Financial services – Personal Identification Number (PIN) management and security (ISO 9564: 2017), Parts 1, 2, & 4;
- Banking – Key management (retail) (ISO 11568: 2005), Parts 1, 2, & 4;
- Core banking – Mobile financial services (ISO 12812: 2017), Parts 1 to 5;
- Financial services – Universal financial industry message scheme (ISO 20022: 2013) Parts 1 to 8; and
- Financial services – Third-party payment service providers (ISO/TR 21941: 2017).

Use Case #3 – Consumer Empowerment and Safety: Digital Food Supply Chains

Background

Due to the complexity of globalized food supply chains, processing technologies, food fraud and international trade, the information associated with food supply chains has never been so important to the safety, integrity and value of what Canadians eat and produce.

The agri-food and agriculture industry is currently undergoing a supply chain digital transformation. A digital supply chain means that the series of activities that are connected – such as the movement of raw materials, goods and parts from the supplier to consumer – and the associated financial, material and information are enabled with digital technology.

These developments present an opportunity to empower consumers, governments and industry to leverage the power of this data. Through trust and transparency, digital technologies could accelerate decision-making processes and drive healthier, safer and economic-based outcomes. Supply chain-level data governance standardization could enable consumers to make informed choices for their families; governments could develop better oversight programs; industry could ensure the quality of their products; and supply chains could respond faster to mitigating and addressing risks.

Consumer Empowerment and Safety: Digital Food Supply Chains Dialogue Sessions

On January 19, 20 and 21, 2021, SCC and the DGSC hosted a series of dialogue sessions with Canadians and stakeholders on the topic of consumer empowerment and safety with a focus on digital food supply chains. Two of the sessions were held in English, while the third was held in French. The sessions were attended by 40 participants from across the country, including representatives from the agri-food/agriculture and technology industries, as well as government and regulatory organizations.

Each session began with a brief presentation by SCC officials on the role of the DGSC and the importance of standards. In addition, a representative from the Canadian Food Inspection Agency (CFIA) provided an overview of the current state of digital transformation in food supply chains and the Safe Food for Canadians Act and Regulations. Participants were then invited to contribute to a conversation focused around two main areas of discussion, namely:

- the current state of digital food supply chains in Canada including existing challenges, opportunities, rules and standards; and,
- the ideal future state, from the desired benefits for consumers to the laws and regulations needed for an effective digital food supply chain framework.

CURRENT STATE AND CHALLENGES

During an interactive whiteboard activity at the outset of the discussions, participants shared their perspectives on the challenges facing digital food supply chains. Ultimately, three recurring and overarching challenges emerged:

1. Lack of a clear value proposition for supply chain participants to encourage acceptance and participation
2. The existence of data silos, and the need for common or interoperable platforms for the transfer of data from numerous sources
3. Transparency, and the need for new and enhanced datasets that facilitate food traceability

Following the whiteboard exercise, participants engaged in small breakout group discussions. When reflecting on the current state of digital food supply chains in Canada, participants generally concluded that greater transparency and traceability are needed to foster consumer trust and safety. Participants also highlighted persistent gaps when it comes to food traceability and suggested not enough time and resources are currently being invested towards traceability efforts to improve the breadth and quality of data available. Finally, in recognition of the challenges posed by the diversity and complexity of the industry, participants expressed the need to ensure the interoperability of digital supply chain tools and platforms across sectors and jurisdictions.

IDEAL FUTURE STATE

When looking ahead to the desired future state of digital food supply chains in Canada, participants expressed the need for practical approaches and incentives for participation. They agreed that the system must enable ease of adoption and access to data for all value chain actors, and that everyone in the value chain should be held accountable to ensure traceability and prevent the loss of data along the chain. In addition, several participants expressed the need for incentives or cost-recovery schemes for value chain actors to buy-in and participate in digital supply chains. Ultimately, participants identified interoperability, privacy and security as key desired outcomes for the standardization of digital food supply chains.

DISCUSSIONS

Current State of Digital Food Supply Chains

In the first half of breakout group discussions, participants were asked to provide their views on the current state of digital food supply chains in Canada.

Recurring themes and key insights from the discussions are summarized below.

Q1.1: What is the current state of the digital food supply chain in Canada?

Theme #1: Consumer trust and safety hinge on greater transparency and traceability.

When thinking about the current state of digital food supply chains in Canada, several participants emphasized the need to improve consumer trust and safety and the importance of making more information available so that consumers can make educated food-buying decisions. It was suggested that consumers have varying levels of confidence in the safety of their food. While some are likely naïve about the products they buy, assuming that everything on the grocery store shelf has been tested for safety, participants noted that other consumers have more questions and higher expectations with regard to the origins of their food, how it is produced and the value chain actors involved.

This topic raised several questions from participants such as:

- What information do consumers need and what are they getting right now?
- What are the key obstacles to overcome in getting this information to consumers?

When discussing consumer trust and safety, participants generally concluded that greater transparency and traceability are needed. While participants feel there is a growing willingness from suppliers and producers to provide more information to consumers about their ingredients and production practices, they said there needs to be a clear benefit for everyone in the industry to do so in a consistent manner.

Participants also highlighted persistent gaps with regard to food traceability, noting the need to better track food products across the full course of the supply chain. It was mentioned that not enough time and resources are currently being invested in traceability efforts to improve the breadth and quality of data available. Some participants speculated that a common standard for traceability would encourage greater innovation and information sharing.

STANDARDIZATION PAIN POINTS

- The current system is not necessarily accessible to all. For example, many suppliers do not possess the necessary technology infrastructure to contribute to this type of data system.
- It is currently difficult for consumers to find information about their food (e.g., traceability). Data should be more broadly available, and this will hold value chain members accountable.

Theme #2: In a diverse and complex industry, cooperation, interoperability and accessibility are critical success factors.

Participants emphasized the diversity and complexity of the agri-food and agriculture industry, noting that significant differences exist across sectors and jurisdictions in Canada and internationally. They suggested that supply chains vary dramatically from dairy to chicken, eggs, produce and other areas of the industry. These differences include how digital supply chain frameworks are being implemented, with some participants pointing out that, while pockets of work are taking place, no uniform standards are being adhered to across the industry.

In light of these differences and the recognition of mounting challenges in ensuring food safety, participants expressed the need to ensure the interoperability of digital supply chain tools and platforms across sectors and jurisdictions. It was noted that a lot of data collection is happening but producers do not have the technical knowledge and skills to bring that data together in order for it to be shared across the whole value chain. It was also suggested that many suppliers would not necessarily have the technology required to contribute to this type of data system, so we need to make sure it is adaptable and accessible to everyone.

Interestingly, some participants indicated that collaboration across the industry has suffered during the pandemic, with one participant saying: “The state of collaboration we were used to before COVID cannot work the same way going forward. This is where we’ll need to reset and rebalance. Right now, we are unbalanced. All supply chains have major variations. There has to be new dialogue about what public health is doing and what we should be doing.”

STANDARDIZATION PAIN POINTS

- There is no clear value proposition. Value chain players do not necessarily understand the value of participating in and contributing to an integrated digital food supply system.
- There is some concern that digitization might act as a barrier or hurdle for interoperability and general connectivity. Incentives are required for a digital shift.
- The state of collaboration in the food supply chain we were used to before the COVID-19 pandemic, cannot work the same going forward.

Theme #3: More consumer-friendly access to information is needed.

Several participants agreed that consumers are becoming increasingly discerning in their preferences when it comes to the foods they buy and eat; however, there is not a standard way for consumers to easily find information about the origins and production methods of their food. One participant suggested the use of scannable QR codes may be a solution; however, standards would be needed to ensure consistency of application and the data available to consumers.

STANDARDIZATION PAIN POINTS

- It is currently difficult for consumers to find information about their food (e.g., traceability). Data should be available, and this could help to hold value chain actors accountable.

Q1.2: What rules, regulations, or standards currently exist, that you are aware of, to regulate the digital food supply chain?

Theme #4: There is a foundation of existing standards and successful first-to-market technology deployments for Canada to build upon.

Participants identified a number of existing standards that are relevant to digital food supply chains, including:

- AG Data Transparent Certification (USA)
- CFIA seed certification platform in support of the Seed Act and Regulations
- DAMA framework (presentation tier, unified data tier)
- CSA Group research on relevant standards, specifically the “Provenance and Traceability Rare Earth” report

In addition, a number of successful ‘first to market’ technology deployments were mentioned in the discussions, which could help to inform future standards, including:

- Agriculture and Agri-food Canada invested in a first-of-its-kind pilot as part of the Canadian Agricultural Strategic Priorities Program to use blockchain to follow locally produced certified soybean seed through production and processing to grocery shelves.
- IBM Food Trust™ is the first blockchain food safety solution that allows transaction partners to confidently and securely share food information, creating a more transparent and trustworthy global food supply chain.
- Microsoft’s technology, known as Farm Beats, uses blockchain, drones and AI to improve productivity and reduce water consumption on farms.

Future State of Digital Food Supply Chains

In the second half of **breakout group discussions**, participants were asked to provide their views on the desired future state of digital food supply chains in Canada.

Recurring themes and key insights from the discussions are summarized below.

Q2.1: What is the ideal future state of the digital food supply chain in Canada?

Theme #5: A pragmatic, value-driven framework is needed for buy-in and participation by all supply chain actors.

When thinking about the design of a digital food supply chain, participants expressed the need for practical approaches and incentives for participation.

In the discussion, some participants suggested that a pragmatic framework should be a guiding principle for the digital food supply chain in Canada. They explained that the approach must not be too cumbersome in process or ambitious in implementation so as to “paralyze” consumers or industries. For example, one participant speculated that, if regulations are too rigid or stringent, there may be unintended consequences for the industry and consumers. One participant summed up the ideal approach as “industry-led, and government-supported.”

Participants agreed that the system must enable ease of adoption and access to data for all value chain actors, and that everyone in the value chain should be held accountable to ensure traceability and prevent the loss of data along the chain. The interface between farmers and processors was highlighted as a key link in the supply chain that must overcome the hurdle of digitization, as paper forms and spreadsheets continue to be common methods of sharing information between these actors.

Another organizing principle suggested by respondents is to “find mutual benefit for collective impact.” To this end, several participants expressed the need for incentives for value chain actors to buy-in and participate in digital supply chains. One participant put forward the idea of paying farmers per head of livestock so they can recover the costs associated with collecting and sharing data. Another participant suggested that consumers may cover the costs for the value added by more information, saying products with more information about their origins or production methods could command a premium price.

Q2.2: What rules, regulations or standards are necessary for a digital food supply chain framework in Canada?

Theme #6: Standards should focus on interoperability, privacy and security.

Participants identified interoperability, privacy and security as key desired outcomes for the standardization of digital food supply chains.

From an interoperability perspective, it was emphasized that all actors in the supply chain, from producers to processors and retailers, need to be continuously involved and engaged to ensure consistency. One participant noted: "All stakeholders need to be brought together and understand the use cases which are constantly evolving and expanding." Some participants expressed the need for rules or regulations that would ensure that data could be accessed across various technologies, platforms and systems. To this end, it was suggested that open standards around APIs would be beneficial.

The imperative for strong privacy and security policies around data storage and transfer was also underscored. Participants were particularly concerned about ensuring that all users of a technology or application are aware of how their information will be shared and with whom. One participant pointed out the challenges for implementation posed by differences in provincial privacy and security legislation and the need for alignment with international standards.

Theme #7: Product certifications should continue to be supported in the transition to the digital food supply chain.

Food product certifications were highlighted as a best practice for educating and informing consumers, and which should continue to be supported in the transition in the digital food supply chain. Participants indicated that putting a certification mark on a food product is a trusted and familiar way for consumers to identify attributes or assurances they want, whether related to country/region of origin or compliance with established organic, environmental or other production standards.

Use Case Working Group Report

The use case group used the DGSC's lifecycle assessment tool to identify standardization issues and/or gaps. A produce flow schematic was used to consider and identify all the actors in the complex supply chain (see visual at end of report). Several recurring challenges were identified and categorized into three themes.

The use case group determined that the issues/gaps previously identified by the four working groups were applicable to the sector. The use case group decided on key questions driving consumers to make purchasing decisions and aligned them to nine key data governance issues.

GENERAL FINDINGS

The complexity of food supply chains (management practices, sourcing of inputs, processing technologies, outbreaks, provincial and international trade, data management and reporting, assurances systems) and increasing demand for trust and transparency means that the information associated with food supply chains has never been so important to the safety, integrity and value of what Canadians eat and produce. With this in mind, the agri-food and agriculture industry is currently undergoing a supply chain digital transformation.

Key Themes:

- Industry digitalization and interoperability;
- Data needs and harmonization; and
- Data access, roles and confidentiality;

1. **Theme 1 – Industry digitalization and interoperability:** Difficulty with industry digitalization stems from the lack of a clear value proposition for supply chain actors to encourage the business case for digitalization and enhanced traceability. When thinking about the ideal future state, the results from the public consultations identified the need for incentives for participating in digital supply chains.

2. **Theme 2 – Data needs and harmonization:** The use case group discussed the need to harmonize data and increase interoperability to enable data exchange. This would improve consumer trust by enabling transparency and providing consumers easy access to the information required when making purchasing decisions. Participants in the public consultation echoed these sentiments around consumer trust and the requirement to improve information access, traceability and transparency along the supply chain.

   The bigger challenge and need with harmonization is to find a way to manage the digital supply chain as a collective effort. The existence of data silos is the current reality of the supply chain. There is a need to enable multilateral relationships and build new services for new actors such as consumers; hence, the applicability of solutions like blockchain.

3. **Theme 3 – Data access, roles and confidentiality:** Collected and available data is currently inaccessible along the supply chain due to the silos where it is collected and the lack of technology infrastructure, in addition to inconsistencies in data quality and reporting. Similarly, available data is not easily accessible to consumers.

There is a need to standardize the key data elements to be captured and determine what needs to be shared. Standardizing roles along the supply chain with respect to data and determining who is allowed to do what within each transaction, their commitments, and incentives needs to be outlined for accountability purposes while protecting confidential business information.

WORKING GROUP FINDINGS

By reviewing the identified issues across the four working groups, in the context of the Consumer Empowerment and Safety Use Case, the use case group identified the following overarching issues: (*the findings are presented by issue and the major issue is bolded*):

1. **Issue 20 (Data Access):** This issue considers the process around data access and usability. Consumer-friendly access to information is required to assist in their purchasing decision-making process. While standardizing data access will give consumers the tools they need to make informed purchasing decisions, a one-size-fits-all approach to standardizing data access may not be beneficial for the industry. Determining data access should be defined by the users of the system.

2. **Issue 11 (Data Collection):** The focus of this issue is on primary data collection. Understanding the purpose, the need and existing mechanisms for quality and integrity during data collection along the supply chain is essential to determine what data should be collected, how data is to be captured and how it is to be shared, to ensure safety and confidence in the data. While some along the supply chain collect data through GS1, others use pen and paper to capture and collect data. This provides a high barrier to rapid digitization and should be considered when standardizing data collection.

3. **Issue 21 (Data Retention):** This issue identifies the need for standardizing a procedure within an organization for retaining information. If a product has been tracked and then removed from stores permanently, how long should the data be kept? The use case group highlighted the need for guidance on data retention and maintenance. However, it noted that defining a set of rules would be too rigid to meet all needs. *(note: the Safe Food for Canadians Regulations (SFCR) outlines how long and where traceability documents are to be kept)*.

4. **Issue 22 (Identity Management):** This issue covers the need to standardize terminology and concepts for identity management to promote a common understanding. Each actor needs to be trusted by the supply chain to be the entity it claims to be. It describes the management of individual identities, their authentication, authorization, roles and privileges across boundaries. Identifying actors that provide data along the supply chain and onboarding new participants to the supply chain in a reliable manner is required to foster and build trust and transparency.

5. **Issue 13 (Discoverability of the Data):** This issue focuses on identifying existing data sets, how to find them, and how to be able to use them. There is a need to standardize where to look for data and how to search for data. While data is being collected along the supply chain, the technical knowledge and skills required to integrate and share available data across the whole value chain is a challenge. Consumers should be able to search and collect information regarding a farm or food processer, for example, in a pragmatic way.

6. **Issue 9 (Data Actor and Data Transaction Roles):** This issue explores the roles of data actors throughout the lifecycle of the supply chain and covers the data management process between data collection and data consumption. Due to the complexity of food supply chains, clarity around roles with respect to data is required. Apart from the typical identified actors, recognizing other value chain participants and understanding the role of consumers will ensure everyone is held accountable, will support traceability and prevent loss of data along the supply chain.

7. **Issue 16 (Metadata Management) and Issue 11 (Data Collection):** Metadata management has strong links with data collection; for this reason, both issues have been combined for the purposes of this report. Metadata management includes collection, management, accessibility and viability of metadata. Establishing the type of meta information/data (i.e., type of identifiers, format or coding system) that is required through the supply chain is important so that supply chain actors use the data. Standardizing the governing principles in providing data descriptors will support the identification of stakeholders collecting data and provide transparency regarding data in the collectors' data management system.

8. **Issue 28 (Data Transparency, Lineage and Traceability):** The focus of this issue is around transparency and traceability of data while being used through its lifecycle. Traceability is a key challenge facing the digital food supply chain in Canada. Understanding how data transactions along the supply chain are logged, who has access to the trail and what is captured can close the persistent gaps with regard to food traceability. Standardizing the minimal information required for collection, including standardizing the data element and attributes, would enable consumers to be better informed and create differentiation in the market. Further standardizing who has access and how seems too restrictive and less voluntary.

9. **Issue 29 (Data Portability and Mobility):** This issue centres around the ability to receive and transmit data between systems without further manipulation. Standardizing which supply chain actors can request a copy of their data to be extracted in digital form, as well as guidance around the removal of data, would be beneficial in preserving exchange of information between systems and would help farmers and producers be less dependent on individual IT providers.

RECOMMENDATIONS

The DGSC should review the findings below from the use case group and public consultations for consideration to be prioritized for standards development. The recommendations are sector specific and not for data governance as a whole. Please note the numbered issues below are from the 35 data governance issues identified by the four DGSC Working Groups.

1. **Issue 20 (Data Access):** Further research is recommended to ensure a standardized approach is beneficial to the agri-food and agriculture sector. It is important to note that a one-size-fits-all approach to third-party data access can make interpretation challenging for different industries. Data access may be best defined by the users of the system.

2. **Issue 21 (Data Retention):** The standardization approach should not set out rules but rather provide guidance around retention and the maintenance of data along the supply chain.

3. **Issue 22 (Identity Management):** There should be a standardized way to uniquely identify all data actors along the supply chain so they can be trusted to be the entities they claim to be.

4. **Issue 13 (Discoverability of the Data):** There should be standardization around the methods in which data can be searched so consumers and others along the supply chain are able to easily find the information they need.

5. **Issue 9 (Data Actor and Data Transaction Roles):** Standardization of roles will ensure that everyone is held accountable to ensure traceability and prevent the loss of data along the supply chain.

6. **Issue 16 (Metadata Management) –** Standardization of the governing principles in providing data descriptors will support the identification of stakeholders collecting data and provide transparency regarding data in the collectors' data management system.

7. **Issue 28 (Data Transparency, Lineage and Traceability):** Standardization of the minimal information to be collected, including the data element and attributes, is crucial. Further standardizing who has access and how seems too rigid and less voluntary. It is important to consider the traceability standards that currently exist, such as the GS1 Global Traceability Standard and the ISO traceability standards (specifically ISO 22005 Traceability in the feed and food chain – General principles and basic requirements for systems design and implementation). These standards are widely used across supply chains and should be taken into consideration by the DGSC.

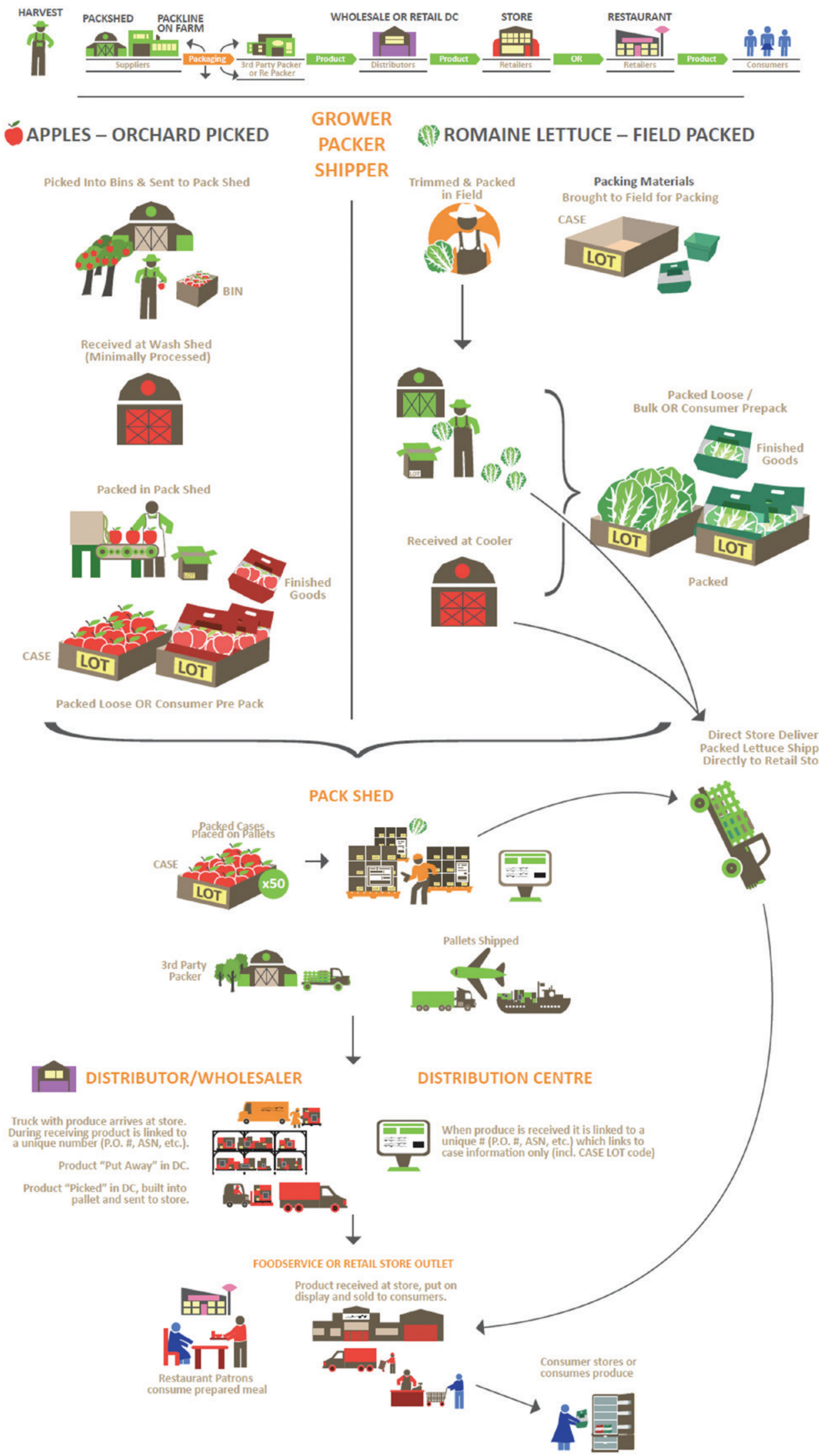
8. Standardization around interoperability, privacy and security are key desired outcomes for the standardization of digital food supply chains.

CONCLUDING COMMENTS

The diversity and complexity of the agri-food and agriculture value chain makes standardization challenging. While standardization could help the industry ensure quality of products, mitigate and address risks (such as in the event of an outbreak) and help consumers make informed decisions, the industry is hesitant about setting rules or using language that regulates rather than provides guidance. The impact of this can halt innovation and have unintended consequences for the sector. It is important to consider the potential impact new data governance standards could have on industries if standards are too ambitious in implementation or too complex in process so as to immobilize consumers or industries.

The use case group appreciates the opportunity to have been asked to do this review. Through its work and feedback from the public consultations, a list of recommendations was identified for consideration for the DGSC. If there are concerns, comments, or questions based on this work, the use case group is happy to re-engage as appropriate.

Traceability Produce Flow Schematic – Developed by the CPMA


HARVEST
PACKSHED
PACKLINE ON FARM
Suppliers
Packaging
3rd Party Packer or Re Packer
Product
WHOLESALE OR RETAIL DC
Distributors
Product
STORE
Retailers
OR
RESTAURANT
Retailers
Product
Consumers
APPLES – ORCHARD PICKED
GROWER
PACKER
SHIPPER
ROMAINE LETTUCE – FIELD PACKED
Picked Into Bins & Sent to Pack Shed
BIN
Received at Wash Shed (Minimally Processed)
Packed in Pack Shed
LOT
Finished Goods
CASE
LOT
LOT
Packed Loose OR Consumer Pre Pack
Trimmed & Packed in Field
Packing Materials Brought to Field for Packing
CASE
LOT
LOT
Packed Loose / Bulk OR Consumer Prepack
Finished Goods
Received at Cooler
LOT
LOT
Packed
Direct Store Delivery Packed Lettuce Shipped Directly to Retail Store
PACK SHED
Packed Cases Placed on Pallets
CASE
LOT
x50
Pallets Shipped
3rd Party Packer
DISTRIBUTOR/WHOLESALER
DISTRIBUTION CENTRE
Truck with produce arrives at store. During receiving product is linked to a unique number (P.O. #, ASN, etc.).
Product "Put Away" in DC.
Product "Picked" in DC, built into pallet and sent to store.
When produce is received it is linked to a unique # (P.O. #, ASN, etc.) which links to case information only (incl. CASE LOT code)
FOODSERVICE OR RETAIL STORE OUTLET
Product received at store, put on display and sold to consumers.
Restaurant Patrons consume prepared meal
Consumer stores or consumes produce

Future Use Case – Children's surveillance and e-Learning systems

Background

As the consultations for the three uses cases wrapped up in January 2021, the DGSC began to receive requests for future use cases that could be part of a Version 2 of the Roadmap. One of these future use cases focuses on Children's surveillance and e-Learning systems, and points to the need for continued vertical discussions on data governance as it impacts different sectors. To support this important topic, SCC, with the support of H+K Strategies, held a two-hour conversation on the topic.

This discussion allowed SCC and participants to learn about Canadian's perspectives and to learn more about work being done in this area. The conversation revolved around two main areas. The first focused on the current state of online surveillance in Canada and its data governance frameworks:

- What are the current challenges for technology governance with regards to online surveillance (i.e., what information is required, how secure is the information, who has access)?
- What rules, regulations, or standards currently exist, that you are aware of, to regulate online surveillance?

The second topic focused specifically on the future of technology governance and online surveillance:

- What is the ideal future situation of online surveillance in Canada (i.e., what are the ideal opportunities, what benefits/risks will result from increased use of online surveillance)?
- What does parental consent look like with the PIPEDA (privacy law) update and with the use of emerging data governance standards?
- What rules, regulations or standards are necessary for a technology governance and online surveillance framework in Canada?

Today, due to COVID-19, in-person interactions have become restricted, so traditional sectors and institutions are having to react immediately to reshape their frameworks to adapt and compete in a digital environment. The pandemic has exposed weaknesses in the area of online surveillance which have become a critical issue as Canadian children adapt and are on-boarded to e-Learning systems.

The lack of data governance standards, enforced privacy regulation and implementation of consistent operational or security procedures in schools exposes children, parents and Canadian society to risks. This is a critical issue, as provinces have traditionally viewed privacy as a cultural point of distinction regionally, and this is contributing to serious cyber security issues.

This is especially apparent with the onboarding of e-Learning systems in schools due to the pandemic. This raises resinous concerns for Canadians related to the processes that mitigate digital identity risks and exposure among schools, teachers, parents and students.

Educational technology (EdTech) has long posed privacy concerns and equality problems. With the increase in EdTech and e-Learning systems to support remote learning during the COVID-19 pandemic, there is a need to develop initiatives and common operational procedures to support online surveillance and mitigate the significant risks associated with digital identity, security and privacy. Schools are often not fully aware of the risks and implications of online privacy and security, such as the sale of student data to third parties for the purpose of advertising, tracking of student activities inside and outside of the classroom, and loss of student autonomy due to ongoing monitoring of their activities. Online surveillance for e-Learning systems needs to become a priority for policymakers, politicians and business leaders to bring online surveillance into government, address privacy and security problems in digitally networked environments, and ensure that individuals who are not part of the various communities in Canada are accommodated.

While there are clear policies at the provincial, school board and national level, there is a lack of enforcement at the school level. For example, education data governance policy in Ontario does exist for Ontario School Records but it does not extend to third-party service providers. Therefore, many applications are not actively reviewed or audited beforehand. EdTech applications are often not vetted by school administrators for privacy compliance, which can result in misleading privacy claims. Combining these EdTech applications with the fact that cyber and physical security policies are inconsistently applied across schools results in an education system leaving children more exposed, parents unaware of the risks, teachers faced with pressure to deliver effective curriculums without understanding the impacts of these applications, and IT administrators stretched to deliver services at the expense of policy mandates. There has been significant regional variation in the K-12 systems in Canada with respect to the implementation of EdTech which has resulted in some platforms and services, such as Zoom and Skype, used for education even if they have not been designed for educational purposes. These types of services and platforms often collect a great deal of personal information about students, such as a student's school, name and use of the platform, which can pose long-term risks to student privacy and autonomy.

In addition, the research study supporting this sector found that most EdTech companies did not provide meaningful consent for parents and notice of risks, nor the data security, transparency and protection of children's e-Learning identifiers (metadata) that is associated with children to satisfy PIPEDA Principle 7, safeguards and meaningful consent notice of risk.

This is a concern for Canadians as it has indicated that e-Learning platforms and education technology companies do not provide meaningful parental consent or best practices for 2 Factor Consent (2FC), referring to both prior notice of risk and notice of consent. Parents are unable to identify risks to their children before data is collected or used. Sufficient best practices as demonstrated by 2FC are important for an e-Learning platform as it ensures the education technologies provide legal parental consent and conform to industry best practices. These concerns are particularly visible in questions related to the security of personal information, where it was found that only one-fifth of the technologies had or provided visible security and data protection policies relevant to Canada.

With the pivot to education through e-Learning platforms and other virtual means to support in-classroom learning, there is a need to evaluate harms to vulnerable children by the virtual platforms used to support the educational sector. Most if not all technologies and e-Learning applications used have not been properly secured to combat and mitigate online surveillance concerns and digital identity risks faced by schools, teachers, students and parents. Ensuring coherence among the policy and operational procedures of education and social media technology in Canada is a critical concern, not only for parents but for Canadian society.

The use of Canadian metadata without consent highlights that service providers have been profiling Canadians' data and aggregating it to build social media products without safeguards to protect Canadians and aggregating data to build products that give service access to this data in contravention of Canadian privacy law, culture,and expectations.

The protection of children's metadata in e-Learning is imperative in mitigating the significant risks posed by factors such as disparate levels of training, different policy across schools and boards, lack of implementation of existing policies and recommendations, and different policy at the federal level and across service providers and operators.

With these challenges in mind, standardization is required for consented online surveillance frameworks to reflect the values of Canadians and to support the needs of children when exposed to online surveillance. This possible future Data Governance use case could champion best practices for the provision of physical and cyber security services and countermeasures for the future in a digital Canada.

CHILDREN'S SURVEILLANCE AND E-LEARNING SYSTEMS SESSION

On February 25, 2021, SCC convened a discussion 23 participants to hear some Canadian perspectives on children's surveillance and e-Learning systems and to find out more about work being done in this area. Facilitated by H+K Strategies, the discussion began with a whiteboard session to get a better understanding of key challenges, followed by two discussion sessions, the first considering the current situation in Canada and the second looking at what an ideal future scenario would be.

Current State of Children's Surveillance and e-Learning Systems

In the first half of the discussion, participants were asked to provide their views on the current state of children's surveillance and e-Learning systems.

Q1.1: What are the current challenges for technology governance with regards to online surveillance (i.e., what information is required, how secure is the information, who has access)?

Theme #1: Definitions

Participants said it is important to have an agreed definition of "online surveillance," as not everyone interprets it the same way. They also noted the importance of distinguishing surveillance from data collection. Generally, surveillance is the monitoring of computer use, activity and data use based on someone's online activity. It is often unregulated and done without consent. But while technology can result in situations of surveillance, there is some legitimate data collection that takes place, such as recording student numbers, names and course information.

Theme #2: Transparency

There should be full transparency so all participants – students, parents, teachers, administrators – clearly understand what data is being collected and why, because without knowing the intended use of data, it is impossible to provide informed consent. Terms and conditions (T&Cs) are often complicated and difficult to understand as they are written in technical or legal language, which also makes it difficult to provide informed consent. T&Cs are often not designed with privacy as a key consideration, so people do not always know what is being done with the data they provide, whether it is being used for purposes other than the one(s) for which it is collected, who is storing their data, or where. It was noted that big companies (mostly American) aggregated data without consent. Participants also pointed out that every actor in a data transaction (actor or subject, student or parent) will need to have access to certain data depending on their role, but these access rights are not always clear.

Theme #3: Consistency

Participants said there is confusion about the different ways educational institutions are using e-Learning tools such as Teams and Zoom, and about the various T&Cs governing those technologies. It is not clear who owns the data in the recordings, including the curriculum, thoughts and information gathered among all the data, or who has access to those recordings. There is no consistent view on what parental consent is, as it does not come from the schools but from the technology companies. Participants wondered if educational institutions understand what is happening and why. It was felt that more information is needed to understand the teacher/administrator perspective by auditing or surveying schoolboards, and that students should be interviewed about their use and understanding of e-Learning tools. The T&Cs for software and systems should also be reviewed to better understand them.

Theme #4: Technology

It was noted that schools had begun to look at e-Learning tools many years ago, but the COVID-19 pandemic accelerated their use. Educators were under intense pressure to deliver online training and therefore adopted tools that were easy to use but not necessarily designed for privacy or compliance. A concern was expressed that technologies that are already approved or in use can take precedence over new technology that could be more appropriate and secure for e-Learning.

Q1.2: What rules, regulations, or standards currently exist, that you are aware of, to regulate online surveillance?

Theme #5: Privacy

Participants cited a number of examples of work already being done that could contribute to the development of appropriate regulations to govern various aspects of online surveillance. These include:

- Self-sovereign Identity (SSI) (also being developed by BC Gov.) https://docs.igrant.io/ssi/
- ISO/IEC 29134:2017 https://www.iso.org/standard/62289.html – Information technology – Security techniques – Guidelines for privacy impact assessment
- ISO/IEC WD TS 27560.2 – Privacy technologies – Consent record information structure
- https://www.iso.org/standard/80392.html
- ISO/IEC 24760-1:2019 – IT Security and Privacy – A framework for identity management – Part 1: Terminology and concepts https://www.iso.org/standard/77582.html
- Publicly Available Standards https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html
- UK Age Appropriate Design Code https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/
- US FERPA (Family Education Rights and Privacy Act)

The Office of the Privacy Commissioner of Canada has guidance on meaningful consent, including a section on Children and Consent – https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

Some participants pointed to the United Kingdom as a jurisdiction working on new standards designed for children. For example, in Q1 2020, the UK government ran a set of decision trees to understand children at different ages, including the risks they face and how to mitigate those risks.

It was noted, however, that any policies and regulations put in place will not be effective if they are not enforceable, particularly as data often travels through other jurisdictions. Canada has strong consent laws, but these might not be enforceable internationally.

Future State of Children's Surveillance and e-Learning Systems

In the second half of the discussion, participants were asked to provide their views on the desired future state of children's surveillance and e-Learning systems.

Q2.1: What is the ideal future situation of online surveillance in Canada (i.e., what are the ideal opportunities, what benefits can consumers/service providers reap from increased use of online surveillance)?

Theme #6: Collaboration

Participants want to see a tailored, easy-to-use environment for parents and educators, designed by Canadians, within a Canadian context. They believe that data generated and collected in Canada must remain in Canada, which will require a reduced dependence on foreign technology companies. There should be an online directory of service and technology providers, so information about them is available to schools and parents. (It was noted that, in the United States, teachers have bypassed their school systems' internal processes and brought apps directly into their classrooms.) One person noted the difficulty within the Canadian confederation when the federal government proposes one set of rules and regulations, but the provinces want to do things differently. Others wondered how the structure could be changed to make things work together.

Theme #7: Security

There is a need to better define the role of technology companies and the access they can have to different types of data. People need to be able to ensure they are consenting in a meaningful way, as they are tracked and traced throughout their lives, and government should have more control over that. There should be ID management when consent is provided by an authorized representative. Cyber security must be considered, including what companies and organizations can do to strengthen protections. The right to be forgotten should be included in any rules and regulations.

Theme #8: Best Practices

Participants want to see best practices shared to help train parents, educational institutions and students. They want children to be at the centre of any governance procedures – the ideal scenario would maximize the control students have over the data they provide to service providers, including being able to opt out of certain uses, particularly those that monetize or commodify data. Systems should be designed with children in mind, made as safe as possible, with privacy, data collection and consent in mind. There should be a clear purpose for data collection, and the use case should be beneficial to the content provider and the end user. One participant noted the work being done by BeaconAI to establish a data privacy receipt that would provide a better understanding of what data is collected and what is done with it.

Q2.2: What does parental consent look like with the PIPEDA (privacy law) update and with the use of emerging data governance standards?

Theme #9: Access

People need to know what their options are when it comes to giving consent, including what the consequences are for not providing consent and what alternatives exist. For example, do students lose the opportunity to take part in e-Learning if they (or their parents) refuse to give their consent? Do teachers lose the right to teach? Can people give partial consent? And if consent is not given, what are the obligations on educational institutions to provide an alternative learning experience?

One participant cautioned against making parental consent the only option. This is often seen as a way to protect children because they are naïve, but sometimes young people have more knowledge of the technology than their parents or want more (or different) data privacy than parents or schools are willing to accept. This requires determining the hierarchy of roles. Currently, children are at the bottom because parents and educational institutions are trying to protect them, but they should also be part of decision making and the comprehensive choice structure. The regulated jurisdictional age of consent for online data collection from children is what should govern parental rights to give consent. The European Union's General Data Protection Regulation (GDPR) approaches this in a child-friendly way, with children typically taking control when they reach the age of 13. There should be connections between parents and children on platforms, through a seamless and intuitive process. There needs to be standardized age-rated content so that it is easy to understand the nature of consent required.

Q2.3: What rules, regulations or standards are necessary for a technology governance and online surveillance framework in Canada?

Theme #10: Security

Participants cited the need for a risk assessment of the sensitivity of data and the impact of collected data. They recognized Bill C-11 is trying to align Canadian rules with the EU's GDPR and the California Consumer Privacy Act (CCPA) but said it still has shortcomings, including that it leaves it to regulators to tell technology companies what to do (it was noted that this is less than ideal, as companies can often "run circles around" regulators). It was also noted that the CCPA does not use standardized justification and does not include specifics on parental consent.

Theme #11: Privacy

Terms and conditions should be designed from the outset with privacy top of mind. Adoption of consent receipts for data should be built into the system. It was suggested the strongest privacy laws in Canada should set the standard for other jurisdictions, with one participant noting that Quebec does a good job to direct T&Cs.

Annex E —

DGSC Membership List

(Note: The employment status and organizational affiliation of participants may have changed during the course of this project.)

DGSC Steering Committee

Category / Role	First Name	Last Name	Title	Organization	P/T	Sector
Academia	Adrian Mark	Thorogood	Academic Associate	CPG Centre of Genomics and Policy McGill University	QC	Health
Academia	Eric M.	Meslin, PhD, FCAHS	President and CEO Senior Fellow, PHG Foundation, Cambridge University	Council of Canadian Academies	ON	General
Academia **WG 2 Co-Chair**	Michel	Girard	Senior Fellow	Centre for International Governance Innovation (CIGI)	QC	General
Academia	Teresa	Scassa	Professor, Faculty of Law, Common Law Section	University of Ottawa	ON	Consulting
Civil Society	Ashley	Casovan	Executive Director	AI Global	ON	Digital Technologies – AI
Civil Society	Aubrey	LeBlanc	CEO	Ontario Building Officials Association, COPOLCO Mirror Committee Chair	ON	Construction
Civil Society	Bianca	Wylie	Independent	Various	ON	Digital Technologies – General

Civil Society **WG 1 Co-Chair**	Carole	Piovesan	Partner and Co-Founder	INQ Data Law	ON	Digital Technologies – Management
Civil Society	Carolyn	Watters	Professor Emeritus	Dalhousie University	ON	Digital Technologies – General
Civil Society	Chantal	Bernier	Counsel	Dentons LLP Senior Fellow, Graduate School of Public and International Affairs, University of Ottawa	ON	Digital Technologies – Management
Civil Society	Jean-Noé	Landry	Executive Director	Open North	QC	Digital Technologies – General
Indigenous Governments and Organizations	Jonathan	Dewar	Executive Director	The First Nations Information Governance Centre	ON	Digital Technologies – Management
Government	André	Loranger	Assistant Chief Statistician (Analytical Studies, Methods, Data Infrastructure), Chief Data Officer	Statistics Canada	ON	Public Services – Federal
Government **DGSC Public Sector Co-Chair**	Anil	Arora	Chief Statistician of Canada	Statistics Canada	ON	Public Services – Federal
Government **WG 3 Co-Chair**	Charles	Taillefer	Director, Privacy and Data Protection Policy Directorate	ISED	ON	Public Services – Federal
Government	Cory	Chobanik	Director	Statistics Canada	ON	Public Services – Federal
Government **WG 2 Co-Chair**	Eric	Rancourt	Director General, Strategic Data Management Branch	Statistics Canada	ON	Public Services – Federal
Government	France	Pégeot	Executive Vice-President	CFIA	ON	Public Services – Federal
Government	Gerard	Peets	ADM, Policy and Results Branch	Infrastructure Canada	ON	Public Services – Federal
Government	Jennifer	Miller	Director General, Strategic Data Management Branch	ISED	ON	Public Services – Federal
Government	Jody	Lobb	Executive Director, Enterprise Strategic Planning	Treasury Board Secretariat	ON	Public Services – Federal

Government	Mark	Schaan	ADM	ISED	ON	Public Services – Federal
Government	Tracy	Wood	COO, Web Digital Office Finance, Treasury Board Secretariat Information Technology Shared Services	Government PEI	PEI	Public Services – Provincial
Industry	Cam	Vilder	Leader, Public Sector	Green Shield Canada (GSC)	ON	Health
Industry	Dana	O'Born	Director, Strategic Initiatives	Council of Canadian Innovators	ON	General
Industry **WG 3 Co-Chair**	Evgueni	Loukipoudis	Chief Technology Officer	Canada's Digital Technology Supercluster	BC	Digital Technologies – General
Industry	Gord	Beal	VP, Research, Guidance and Support	Chartered Professional Accountants Canada (CPA)	ON	Financial Services
Industry **WG 4 Co-Chair**	Grace	Abuhamad	Research Program Manager, Trustworthy AI	ServiceNow	QC	Digital Technologies – AI
Industry **WG 1 Co-Chair**	Joni	Brennan	President	Digital ID and Authentication Council of Canada (DIACC)	ON	Digital Technologies – Management
Industry **WG 4 Co-Chair**	Maithili	Mavinkurve	COO	Sightline Innovation	ON	Digital Technologies – AI
Industry **DGSC Private-Sector Co-Chair**	Philip	Dawson	Digital Policy Advisor Public Senior Policy Counsel	Consultant Responsible AI Institute (RAI)	QC	Digital Technologies – AI
Standardization	James (Jim)	MacFie	National Standards Officer Mirror Committee Chair JTC 1 TC Information Technology Canadian Chair of MC to JTC 1/SC 42 Artificial Intelligence Canadian Vice Chair to ISO/TC 307 on Blockchain and related technologies	Microsoft Canada	ON	Digital Technologies – General
Standardization	Maike	Luiken	President	IEEE Canada	ON	Electronics
Standardization	Mary	Cianchetti	President of Standards	CSA Group	ON	General

Use Case Working Groups

Use Case #1 – Community Health Data	**Eric Sutherlan (Chair)** Executive Director, Pan-Canadian Health Data Strategy, Corporate Data and Surveillance Branch, Public Health Agency of Canada **Allie Harris** Vice President and Chief Data Officer, Scotiabank	**Sheriff Abdou** Chief Data Officer, Public Health Agency of Canada **Eric Rancourt** Director General, Strategic Data Management, Statistics Canada **Michael Nusbaum** President, MH Nusbaum & Associates Ltd.
Use Case #2 – Digital Identity and Open Banking	**The Honourable Colin Deacon, Senator (Co-Chair)** Senate of Canada **Joni Brennan (Co-Chair)** President, Digital Identification and Authentication Council of Canada (DIACC) **Steve Boms** Executive Director, Financial Data and Technology Association (FDATA) **Gene DiMira** Chief Identity Officer, The AML Shop **Franklin Garrigues** Vice President, Digital Channels, TD Bank **Karim Gillani** General Partner, Luge Capital **Jim Hinton** Founder, Own Innovation	**Keith Jansa** Executive Director, CIO Strategy Council **Rene McIver** Chief Security Officer, SecureKey **Kevin Morris** Strategy & Programs Director, Large Credit Union Council (LCUC) **Mike Penner** Chief Operating Officer, VoPay **Sylvie Tessier** Member, Department Audit Committee, Office of the Superintendent of Financial Institutions **Peter Watkins** Program Executive, Institute for Citizen-Centred Service
Use Case #3 – Consumer Empowerment and Safety: Digital Food Supply Chains	**Brian Kowaluk (Chair)** Senior Analyst, Information Management and Risk, Canadian Food Inspection Agency **Evgueni Loukipoudis** Chief Technology Officer, Canada's Digital Technology Supercluster **Geoff Isaacs** Project Leader, Canadian Food Inspection Agency **Jane Proctor** Vice President & Issue Management, Canadian Produce Marketing Association **Joe D'Urzo** Senior Director, Data Operations, Loblaw Companies Ltd.	**Maria Paulina Forero, MSc.** Bioresource Engineer, Agri Industrial Engineer Sector Specialist, Cross Sectoral Issues, Industry Engagement Division, Agriculture and Agri-Food Canada **Michael Gibbons** Co-Founder and VP Product Development, Provision Analytics **Nilos Korodimas** Sector Specialist, Cross Sectoral Issues, Market and Industry Services, Agriculture and Agri-Food Canada **Robyn Edwards** National Manager, Results, Assessment & Measurement, Canadian Food Inspection Agency **Shubh Singh, MBA** Business Development at Accu-Label International

DGSC Membership (excluding the Steering Committee)

Organization	First Name	Last Name	Title	P/T	Category	Sector
	Yassen	Atallah	Policy Analyst		Government	Health
	Stefano	Heguy	Student	ON	Academia	
	Ruben	Sardaryan		ON	Industry	Digital Technologies – General
Capgemini	Tina	Chakrabarty	Director of Insights and Data, Financial Services	ON	Industry	Digital Technologies – Management
Royal Architectural Institute of Canada (RAIC)	Louis	Conway	MRAIC, Architect AIBC	BC	Civil Society	Construction
Alberta Gaming, Liquor and Cannabis	Galina	Rachkova	Data Architect	AB	Government	Public Services – Provincial
Alexis Nakota Sioux Nation	Corrine	St. Dennis	Accreditation Coordinator	AB	Standardization	
Alliance of Canadian Building Officials Association	Matthew	Farrell	Vice President	ON	Government	Construction
Arup Canada Inc.	Justin	Trevan	Associate Principal	ON	Industry	
Associated Engineering Alberta	Judy	Yu	Roads Manager	AB	Industry	Consulting
BlackBerry	Takashi	Suzuki	Senior Director, Standards and IP Development	ON	Industry	Communications
Bloomberg LP	Richard	Beatch	Semantic Architect	US	Industry	Communications
BlueShore Financial	Janet	Burgess	VP Retail Banking/AVP BI Solutions	BC	Industry	Financial Services
BlueShore Financial	Fred	Cook	CIO	BC	Industry	Financial Services
BlueShore Financial	Rup	Parmar	Vice President, Business Technology Development	BC	Industry	Financial Services
British Columbia Lottery Corporation (BCLC)	Sarah	Marshall	Data Governance Officer	BC	Industry	
Cabrian Credit Union	Diane	Bilodeau	SVP, Member Engagement & Business Intelligence	MB	Industry	Financial Services
Canada Border Services Agency	Evelyn	Duberry	Senior Program Advisor	ON	Government	Public Services – Federal
Canada Bridges Consulting; CIGI	Marsha	Cadogan	CIGI Fellow, Lawyer, IP and Trade Consultant	ON	Civil Society	Consulting
Canada Health Infoway	Beverly	Knight	Manager Medication Standards	MB	Civil Society	Health
Canada Life	Gladiola	Stringa	Director- Enterprise Data	ON	Industry	Financial Services

Canadian Air Transport Security Authority (CATSA)	Gail	McAuliffe	Senior Advisor, Data Management	ON	Government	Public Services – Federal
Canadian Dental Association	Dean	Smith	Manager, Information Technology	ON	Industry	Health
Canadian Dental Association	Benoit	Soucy	Director Clinical and Scientific Affairs	ON	Industry	Health
Canadian Food Inspection Agency	Andrew	Maw	Chief Data and Risk Officer	ON	Government	Public Services – Federal
Canadian Institute for Health Information	Finnie	Flores	Program Consultant (Standards) & Reference Data Steward	ON	Civil Society	Health
Canadian Institute for Health Information	Rachel	Hemeon	Program Lead, Data Governance and Standards Office	ON	Civil Society	Health
Canadian Institute for Health Information	Eric	Sutherland	Executive Director, Data Governance Strategy	ON	Civil Society	Health
Canadian Medical Protective Association	Om	Patel	External Relations Analyst	ON	Civil Society	Health
Canadian Medical Protective Association	Daniel	Tardif, MD	Director, Regional Affairs	ON	Civil Society	Health
Canadian Mortgage and Housing Corporation	Joel	Sango	Specialist of Survey Statistics	ON	Government	Public Services – Federal
Canadian Research Insights Council	John	Tabone	Chief Administrative Officer	ON	Industry	General
Change Max Consulting	Sherry	Hodge	Global Change Management Leader	BC	Industry	Consulting
Chartered Professional Accountants Canada (CPA)	Gord	Beal	Vice President, Research, Guidance & Support	ON	Industry	Financial Services
Chartered Professional Accountants Canada (CPA)	Michael	Lionais		ON	Industry	Financial Services
CIBC	Navjit	Singh	Senior Manager, AML Analytics	ON	Industry	Financial Services
Canadian Institute for Health Information	Paulo	Domingues	Manager, Architecture and Standards	ON	Government	Health
Canadian Institute for Health Information	Claudiu	Grecu	Data Architect	ON	Government	Health
CIO Strategy Council	Keith	Jansa	Executive Director	ON	Standardization	Digital Technologies – General
CIO Strategy Council	Matthew	MacNeil	Director of Standards and Technology	ON	Standardization	General

City of Winnipeg	Chris	Klos	Manager, Corporate Asset Management Office, OFFICE OF THE CAO INFRASTRUCTURE PLANNING OFFICE	MB	Government	Public Services – Municipal
Cloud Perspectives	Steven	Woodward	CEO	ON	Industry	Digital Technologies – Management
CloudOps	Ian	Rae	CEO	QC	Industry	
Cogentas inc.	Luc	Poulin	CEO	QC	Industry	Digital Technologies – Management
Council of Canadian Innovators	Dana	O'Born	Director, Strategic Initiatives |	ON	Industry	General
CSA Group	Stephen	Michell	Project Manager ICT Standards	ON	Standardization	General
Correctional Service Canada (CSC)	Michael	Elmore	Director of Enterprise Data and Information Management	ON	Government	
Cybersecurity Research Lab	Annegret	Henninger	Project Manager	ON	Academia	Digital Technologies – General
Denologix	Palle	Johnson	Managing Director Public Sector	ON	Industry	Digital Technologies – AI
Department of National Defence	Julia	Dick	Junior Digital Policy Analyst	ON	Government	Public Services – Federal
Desjardins	Elisabeth	Diop	Senior Advisor	QC	Industry	Financial Services
Digital ID and Authentication Council of Canada (DIACC)	Joni	Brennan	President	ON	Industry	Digital Technologies – Management
Environment and Climate Change Canada (ECCC)	Elisabeth	Siré	Economist/Data Governance Analyst	QC	Government	Public Services – Federal
Edge Imaging	Jordan	Moore	VP Marketing and Product	ON	Industry	Services
Edge Imaging	Mike	Watkinson	CTO and CPO	ON	Industry	Services
EllisDon	Rosemarie	Lipman	CIO & SVP, Enterprise Intelligence	ON	Industry	Construction
EllisDon	Patrick	To	Manager, Insight and Analytics	ON	Industry	Construction
Environics Analytics	James	Smith	Chief Compliance and Privacy Officer	ON	Industry	Services
Equifax Canada	Ajay	Handa	Chief Data Officer	ON	Industry	Financial Services
Equifax Canada	Yassir	Jiwan	Digital Innovation Lead	ON	Industry	Financial Services

Equifax Canada	Cris	Krnjeta	Data Analytics		Industry	Financial Services
Excelar Technologies	Colin	Quon	CEO	BC	Industry	Consulting
Financial Data and Technology Association of North America (FDATA)	Steven	Boms	Executive Director	US	Industry	Financial Services
FormAssembly	Beenish	Saeed	Sales Development Representative	ON	Industry	Services
George Brown College	Andres	Ponton	Student	ON	Academia	
Government of BC, Ministry of Health	Noushin	Nabavi	Economist	BC	Government	Public Services – Provincial
Government of Saskatchewan Ministry of Corrections, Policing and Public Safety; Ministry of Justice and Attorney General	Yashu	Bither	Director, Business Intelligence & Data Analytics	SK	Government	Public Services – Provincial
Green Shield Canada (GSC)	Adam	Aspinall	Manager, Data Insights & Analytics	ON	Civil Society	Services
H2O.ai	Bahador	Khaleghi	Customer Data Scientist	ON	Industry	
Health Canada	Peggy	Ainslie	Director	ON	Government	Health
Health Canada	Jenny	Bunning	Policy Analyst	ON	Government	Health
Health Canada	Ben	Diepeveen	Policy Analyst	ON	Government	Health
Health Canada	Jane	Kolbe	Senior Advisor	ON	Government	Health
Health Canada	Brett	Taylor	Policy Analyst	ON	Government	Health
Holt Renfrew	Kristina	Smith	Corporate Privacy Officer	ON	Industry	Retail
HSBC Bank Canada	Matthew	Dickinson	Chief Data Officer	BC	Industry	Financial Services
Hydro Quebec	Sanaa	Achaiba	Business Intelligence Advisor	QC	Industry	Public Services – Provincial
Independent Electricity System Operator (IESO)	Lisa	Barnet	Senior Legal Counsel and Privacy Officer	ON	Government	Public Services – Provincial
Independent Electricity System Operator (IESO)	David	Chong Tai	Senior Manager, Smart Metering	ON	Government	Public Services – Provincial
Independent Electricity System Operator (IESO)	Sorana	Ionescu	Director, Smart Meeting	ON	Government	Public Services – Provincial
Independent Electricity System Operator (IESO)	Erin	Williams	Supervisor, Information Governance	ON	Government	Public Services – Provincial

Information and Communications Technology Council	Rob	Davidson	Director, Data Analytics	ON	Industry	Communications
Information Privacy and Archives Division	John	Roberts	Chief Privacy Officer and Archivist of Ontario	ON	Government	Public Services – Provincial
Infoset	Varinder	Sembhi	Managing Partner	ON	Industry	
Infrastructure Canada	Lucy	Opsitnik	Data Manager	ON	Government	Public Services – Federal
Interac	Aruna	Dorai	Director	ON	Industry	Financial Services
ISED	Dashiell	Dronyk	Policy Advisor, Privacy and Data Protection Policy Directorate	ON	Government	Public Services – Federal
ISED	Jacqueline	Jones	Policy Advisor, Privacy and Data Protection Policy Directorate	ON	Government	Public Services – Federal
KPMG	Najib	Bounouane	Manager, Information and Data Governance	QC	Industry	Services
KPMG	Catherine	Nadeau	Senior Manager, Information Governance	QC	Industry	Services
Labour Program – Employment and Social Development Canada (ESCD)	Jason	Maurice	Senior Policy Analyst	QC	Government	Public Services – Federal
Labour Program – Employment and Social Development Canada (ESCD)	Abhinav	Rao	Data Statistical Analysis Officer	QC	Government	Public Services – Federal
Labour Program – Employment and Social Development Canada (ESCD)	David	Santos	Analyst	QC	Government	Public Services – Federal
Large Credit Union Coalition	Kevin	Morris	Strategy and Programs Director	ON	Industry	Financial Services
LifeSciences BC	Wendy	Hurlburt	President & CEO	BC	Industry	General
Loblaw Companies Ltd.	Alessandra	Bresani	Chief Privacy Officer	ON	Industry	Retail
Loblaw Companies Ltd.	John	Nicodemo	Vice President, Data Engineering	ON	Industry	Retail
M.H Nusbaum & Associates Ltd.	Michael	Nusbaum	President	BC	Industry	Health
Manitoba Public Insurance	Daniel	Faingold	Manager, Business Analytics	MB	Government	Financial Services
Manitoba Public Insurance	Lawrence	Lazarko	Director, Information Technology	MB	Government	Financial Services

Manitoba Public Insurance	Divya	Polavaram	Manager	MB	Government	Financial Services
Mapador	Sam	Malek	Chief Technology Officer	ON	Industry	Digital Technologies – General
Mature-ITSM Inc.	Andre	Boutin	Digital governance consultant	QC	Industry	Digital Technologies – Management
McMaster University / Canadian Research Data Centre Network	Michael	Veall	Professor of Economics/Principal Investigator	ON	Academia	Digital Technologies – General
McMaster University / Vector Institute	Ranil	Sonnadara	Special Advisor to the Vice President (Research) / Associate Professor	ON	Academia	
Minerva Intelligence Inc.	Jake	McGregor	Chief Operating Officer	BC	Industry	Digital Technologies – AI
N/A	Vasiliki (Vass)	Bednar	Private Citizen	ON	Civil Society	Digital Technologies – General
N/A	Jeremy	Depow	Independent	ON	Industry	Digital Technologies – Management
NetGovern	Pierre	Chamberland	CEO	QC	Industry	Digital Technologies – Management
Newcomp Analytics and University of Toronto	Mareena	Mallory	Data Scientist and Adjunct Lecturer	ON	Academia	Digital Technologies – General
Newport Thomson	Derek	Lackey	Managing Director	ON	Industry	Digital Technologies – Management
Northern Credit Union	Chris	Armenti	AVP – Business Solutions	ON	Industry	Financial Services
OACIQ	Dominique	Derome	Vice President – Finance, IT and Business Processes	QC	Government	
OACIQ	Caroline	Simard	Vice President – Governance	QC	Government	
Ontario Building Officials Association, and City of Windsor Building Department	Leslie	Wright	Digital Transformation Specialist	ON	Government	Public Services – Municipal
Octane Biotech Inc.	Chaitanya	Baliga	Head of Quality	ON	Industry	Health
Office of the Privacy Commissioner of Canada	Thibault	Lacroix	Manager, Information Management Programs and Services	ON	Government	Public Services – Federal
Ontario Lottery and Gaming Corporation	Allie	Harris	Director, Enterprise Information Governance	ON	Government	Public Services – Provincial

Ontario Tech University	Andrea	Slane	Associate Professor	ON	Academia	General
Open City Network	Andy	Best	Executive Director	ON	Civil Society	Digital Technologies – AI
Open North Applied Research Lab	Steve	Coutts	Research Analyst	QC	Civil Society	Digital Technologies – General
Opris & Associates Inc.	Candid	Opris	Principal and Managing Partner	ON	Industry	
Own Innovation	Jim	Hinton	Lawyer, Patent & Trademark Agent	ON	Industry	Consulting
Payments Canada	Craig	Borysowich	Principal, Integration & Standards	ON	Industry	Financial Services
Payments Canada	Judy	Li	Manager, Information and Data Analytics	ON	Industry	Financial Services
PBC & Associates	Paul	Cotton	Founder / Owner	BC	Industry	Digital Technologies – General
PEI Department of Finance, IT Shared Services	Nan	Court	Manager of Data Services	PEI	Government	Public Services – Provincial
PEI Department of Finance, IT Shared Services	Roman	Embleton	Data Architect	PEI	Government	Public Services – Provincial
PHAC	Rita	Finley	Senior Policy Analyst, Office of the Chief Science Officer	ON	Government	Public Services – Federal
Plaid	John	Pitts	Head of Policy	US	Industry	Financial Services
Plaid	Ben	White	Policy R&D	US	Industry	Financial Services
Portag3 Ventures	Ben	Harrison	Partner, Head of Partnerships and Policy	ON	Industry	Financial Services
Power Financial Corporation	Pierre	Piché	Vice President	QC	Industry	Financial Services
Professional Petroleum Data Management Association	Trudy	Curtis	CEO	AB	Industry	Energy
Protein Industries Canada	Ken	Sackley	CIO – Head of Data	ON	Industry	Health
PSD Research, Consulting, Software	Matthew	Dawe	Vice President	ON	Industry	Consulting
PSD Research Consulting Software	Tyler	Sutton	General Manager of Research and Marketing	ON	Industry	Consulting

Public Health Agency of Canada	Susan	Ternan	Data Partnerships and Innovation Hub	ON	Government	Health
Public Sector Digest	Chris	Vanderheyden	Senior Asset Management Consultants	ON	Industry	Consulting
PwC	Cristina	Onosé	Lead, Privacy Advocacy and Thought Leadership	ON	Industry	Services
Quantum-Safe Canada	Bill	Munson	Director, Research and Policy Analysis	ON	Academia	Digital Technologies – Management
Questrade	Ernani	Cecon	Director, Enterprise Architecture	ON	Industry	Financial Services
RBC	Lisa Marie	Daulby	Director, Enterprise Data Policy Governance	ON	Industry	Financial Services
RBC	Don	de la Paz	Vice President, Information Management Risk, Chief Data Office	ON	Industry	Financial Services
RBC	Ajinkya	Kulkarni	Senior Director, Data Science	ON	Industry	Financial Services
RBC	Catherine	Stephen	Senior Counsel	ON	Industry	Financial Services
Régie de l'assurance maladie du Québec	Denis	Côté	Conseiller en architecture d'entreprise – Volet information	QC	Government	Public Services – Municipal
Research Data Canada	Mark	Leggott	Executive Director	ON	Civil Society	Services
Retail Council of Canada	Kate	Skipton	Senior Policy Analyst	ON	Industry	Retail
Risk Management Association Toronto/ CGG Consulting	Stella	Cabrera	President/Founder	ON	Industry	Financial Services
SCC MC ISO/PC 317	Graham Rae	Dulmage	Chair	ON	Standardization	Consulting
Secrétariat du Conseil du trésor (SCT)	Marc	Vézina	Directeur de l'architecture d'entreprise gouvernementale	QC	Government	General
SecureKey Technologies	Rene	McIver	CSO/CPO	ON	Industry	Digital Technologies – Management
SecureKey Technologies	Eric	Swedersky	Senior Vice-President, Delivery and Public Sector	ON	Industry	Digital Technologies – Management
Service New Brunswick	Erin	Hardy	Chief Privacy Officer	NB	Government	Public Services – Provincial
Shaw Communications	Sangeetha	Varghese	Manager, Data Governance & Quality	AB	Industry	Communications

SiMPACT	Stephanie	Robertson	Founder and CEO	ON	Industry	Financial Services
Slack Consulting	Ellen	Brown	Business Intelligencec Analyst	ON	Industry	Consulting
Smart City	Steve	Czajka	Manager	ON	Government	Digital Technologies – AI
Smart Species	Mark	Lizar	CEO	ON	Industry	Consulting
Social Sciences and Humanities Research Council	Ariadne	Legendre	Manager – Corporate and Business Analytics	ON	Government	General
Sparkgeo Consulting Inc.	James	Banting	Developer	BC	Industry	Consulting
Statistics Canada	Tom	Dufour	Director General, Strategic Data Management Branch	ON	Government	Public Services – Federal
Statistics Canada	Sevgui	Erman	Director, Data Science Division	ON	Government	Public Services – Federal
Statistics Canada	Julie	Trépanier	Director, Data Integration Infrastructure Division	ON	Government	Public Services – Federal
Sun Life Financial Canada	Paul	Mendes	Senior Director of Data Governance	ON	Industry	Financial Services
Treasury Board of Canada Secretariat, Office of the CIO	Omar	Bitar	Advisor (Enterprise Data & AI)	ON	Government	Public Services – Federal
TD Bank Group	Jennifer	Gibbs	Chief Data Officer	ON	Industry	Financial Services
TD Insurance	Sophiya	Varghese	Senior Manager, Data Governance, Data & Insights	QC	Industry	Financial Services
Tehama Inc.	Karen	Chase	Director, Industry & Government Programs	ON	Industry	Digital Technologies – General
TELUS	Jesslyn	Dymond	Responsible AI Specialist	ON	Industry	Communications
TELUS	Elena	Novas	Director, Privacy & Innovation	ON	Industry	Communications
TELUS Communications	Carine	Botturi	Director – Risk Management, TELUS Data & Trust Office	QC	Industry	Communications
Computer Research Institute of Montreal	Fehmi	Jaafar	Cyber Security Researcher	QC	Academia	Digital Technologies – General
Thomson Reuters	Cormac	Brady	CTO Platform & Content Technology	US	Industry	Communications
ToP KaTS Consulting	Michael	Lamoureux	President	NS	Industry	Consulting

Toronto Region Board of Trade	Thomas	Goldsmith	Policy Director, Innovation and Technology	ON	Industry	General
Trans Union of Canada, Inc.	Heather	Burke	Senior Manager Data Management	ON	Industry	
Trans Union of Canada, Inc.	Johanna	FitzPatrick	Legal Counsel and Privacy Officer	ON	Industry	
Trans Union of Canada, Inc.	Iain	Page	Advisor, Data Strategy	ON	Industry	
Trans Union of Canada, Inc.	Alison	Paisley	Manager – Data Acquisitions	ON	Industry	
Transport Canada	Dominic	Canuel	Manager, Data Management	ON	Government	Public Services – Federal
Treasury Board of Canada Secretariat	Jason	Blackwell	Senior Strategist – Office of the Chief Information Officer of Canada (OCIO)	ON	Government	
Treasury Board of Canada Secretariat	Michael	Goit	Director, Digital Identity	ON	Government	Public Services – Federal
Treasury Board of Canada Secretariat	Dawn	Hall	Advisor	ON	Government	
TrustBIX Inc.	Tom	Ogaranko	Chief Innovation Officer	AB	Industry	Digital Technologies – General
ULC Standards	Gillian	Wintonic	Project Manager	ON	Standardization	General
University of Guelph	Rozita	Dara	Assistant Professor	ON	Academia	Digital Technologies – Management
University of Victoria	Yvonne	Coady	Professor	BC	Academia	Digital Technologies – General
UrtheCast	William	Parkinson	Technical Product Manager	BC	Industry	Digital Technologies – General
Valencial IIP Advisors Ltd.	Michael	Power	Managing Director, Privacy	ON	Industry	Digital Technologies – Management
Vector Institute	Andrea	Smith	Director, Health Data Partnerships	ON	Academia	Digital Technologies – AI
VersaFile Inc.	Darren	Peloso	CTO	BC	Industry	Digital Technologies – General
VoPay International Inc.	Mike	Penner	Chief Operating Officer	BC	Industry	Financial services
WMC	Mike	Hughes	Affiliate	AB	Industry	Consulting
WSP Canada	Lucy	Casacia	Vice President, Smart Solutions	ON	Industry	Digital Technologies – General

DGSC Secretariat

Role	First Name	Last Name	Title	Organization
DGSC Secretary	Anneke	Olvera	Director, Program and Operations, Strategy and Stakeholder Engagement	Standards Council of Canada
DGSC Secretariat	Brendan	McManus	Manager, Innovation	Standards Council of Canada
DGSC Secretariat	Alexandra	Wells	Project Manager, Innovation	Standards Council of Canada
WG1 Secretary	Alex	Héroux	Sector Specialist, Innovation	Standards Council of Canada
WG2 Secretary	Martin-J	Beaulieu	Chief, International Cooperation and Methodology Innovation Centre	Statistics Canada
WG3 Secretary	Andrew	Kostruba	Project Manager	CSA Group
WG3 Secretary	Edwin	Ndatuje	Sector Specialist, Innovation	Standards Council of Canada
WG4 Secretary and Use Case #1 – Community Health Data Secretary	Marta	Janczarski	Sector Specialist, Innovation	Standards Council of Canada
Use Case #2 – Digital Identity and Open Banking Secretary	Dominik	Brejta	Sector Specialist, Innovation	Standards Council of Canada
Use Case #3 – Consumer Empowerment and Safety: Digital Food Supply Chains Secretary	Hana	Qowrah	Sector Specialist, Innovation	Standards Council of Canada
Lead Research and Compendium Developer	Diane	Liao	Program Manager, Research	Standards Council of Canada
Research and Compendium Developer	Inbal	Marcovitch	Special Advisor, CEO Office	Standards Council of Canada

Annex F —

Glossary of Acronyms and Abbreviations

Acronym	Description
AI	Artificial Intelligence
ANSI	American National Standards Institute
API	Application Programming Interface
ASCE	American Society of Civil Engineers
ASTM	American Society for Testing and Materials
AWWA	American Water Works Association
BSi	British Standards Institution
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CGSB	Canadian General Standards Board
CHIMA	Canadian Health Information Management Association
CIE	International Commission on Illumination
Cihi	Canadian Institute for Health Information
CIOSC	CIO Strategy Council
CLSI	Clinical and Laboratory Standards Institute
CSA	Canadian Standards Association
C4DC	Contracts for Data Collaboration
DAMA	Data Management Association
DCAM	Data Management Capability Assessment Model
DGSC	Data Governance Standardization Collaborative
DIACC	Digital ID and Authentication Council of Canada
DIN	German Institute for Standardization
DS	Danish Standards Foundation
EDMC	Enterprise Data Management Council

EdTech	Education Technology
EHR	Electronic Health Record
ETSI	European Telecommunications Standards Institute
FNIGC	First Nations Information Governance Centre
GDPR	General Data Protection Regulation
GOST	Gosstandart Standards
HIMSS	Healthcare Information and Management Systems Society
IAPP	International Association of Privacy Professionals
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IHS	Information Handling Systems
IoT	Internet of Things
IT	Information Technology
ITU-R	International Telecommunication Union – Radiocommunications Sector – Recommendations
ITU-T	International Telecommunication Union – Telecommunication Standardization Sector
ISED	Innovation, Science and Economic Development Canada
ISO	International Organization for Standardization
JTC 1	Joint Technical Committee 1
LOINC	Logical Observation Identifiers Names and Codes
MFI	Metamodel Framework for Interoperability
MDR	Metadata Registry
ML	Machine Learning
NCBI	National Center for Biotechnology Information
NEMA	National Electrical Manufacturers Association
NIST	National Institute of Standards and Technology
NFPA	National Fire Protection Association
PII	Personally Identifiable Information
PIPEDA	Personal Information Protection and Electronic Documents Act
PTAC	Provincial Territorial Advisory Committee
SCC	Standards Council of Canada
SDO	Standards Development Organization
SNZ	Standards New Zealand
ULC	Underwriters Laboratories of Canada
W3C	World Wide Web Consortium
2FA	Two-factor Authentication

Annex G —

Methodology for Developing the DGSC Standards Landscape

The roadmap's focus is from a data governance life-cycle perspective, which is complex and dynamic, undergoing continual evolution and adaptation, with many parties involved. Activities for the development of the roadmap have been framed under four broad domains: (1) Foundations of Data Governance, (2) Data Collection, Organization and Grading, (3) Data Access, Sharing and Retention, and (4) Data Analytics, Solutions and Commercialization. Within those domains, broad topical areas of relevance to standards and conformance programs for data governance have been identified.

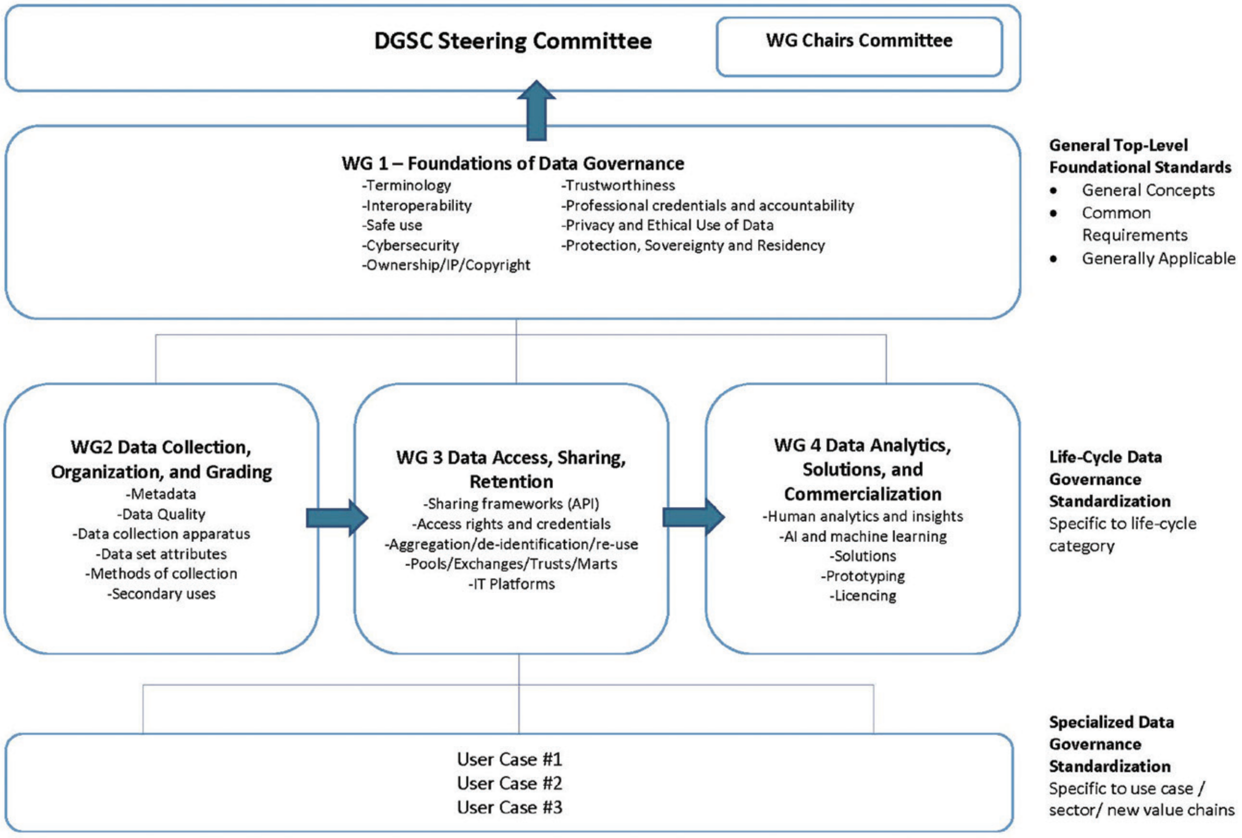
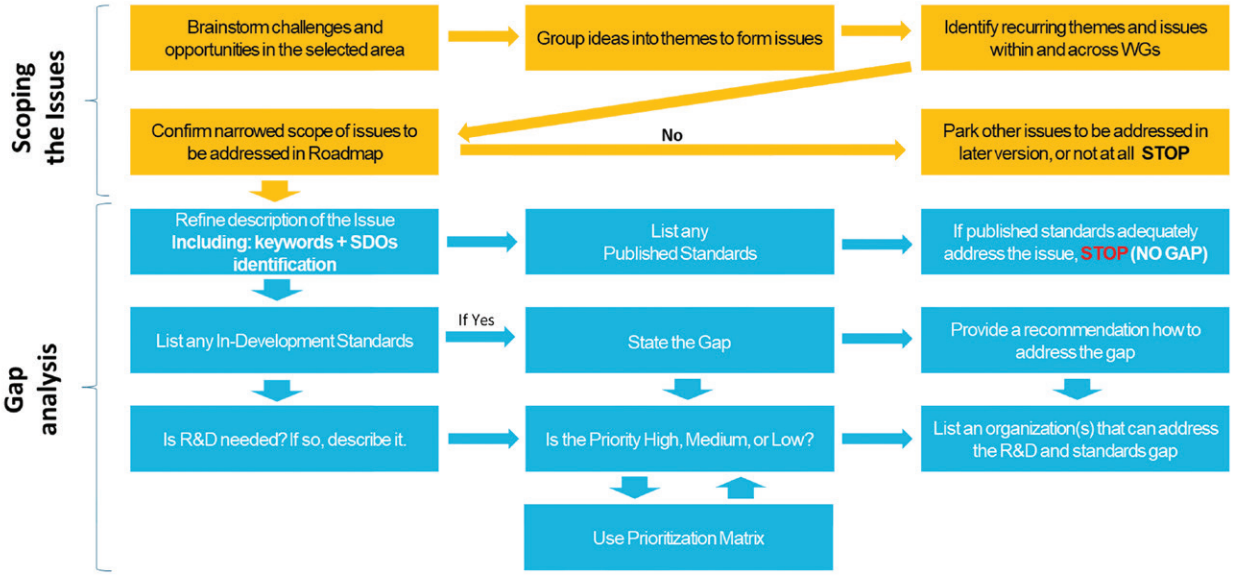

DGSC Steering Committee
WG Chairs Committee
WG 1 – Foundations of Data Governance
-Terminology
-Interoperability
-Safe use
-Cybersecurity
-Ownership/IP/Copyright
-Trustworthiness
-Professional credentials and accountability
-Privacy and Ethical Use of Data
-Protection, Sovereignty and Residency
General Top-Level Foundational Standards
• General Concepts
• Common Requirements
• Generally Applicable
WG2 Data Collection, Organization, and Grading
-Metadata
-Data Quality
-Data collection apparatus
-Data set attributes
-Methods of collection
-Secondary uses
WG 3 Data Access, Sharing, Retention
-Sharing frameworks (API)
-Access rights and credentials
-Aggregation/de-identification/re-use
-Pools/Exchanges/Trusts/Marts
-IT Platforms
WG 4 Data Analytics, Solutions, and Commercialization
-Human analytics and insights
-AI and machine learning
-Solutions
-Prototyping
-Licencing
Life-Cycle Data Governance Standardization
Specific to life-cycle category
User Case #1
User Case #2
User Case #3
Specialized Data Governance Standardization
Specific to use case / sector/ new value chains

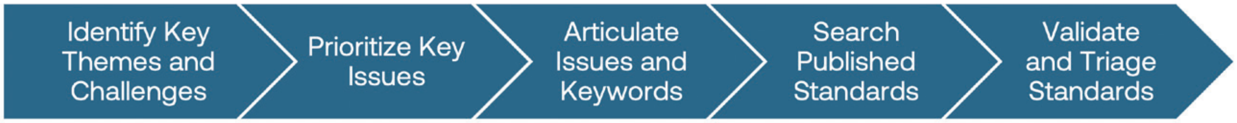
Diagram 1: Structure of DGSC and Roadmap

Following a Phase 1 kickoff meeting in January 2020, where working groups voted and confirmed priority areas for the first version of the roadmap (see diagram 2), the working groups held online meetings every two weeks to describe and scope the key issues, inventory existing standards, conduct the gap analysis and draft the roadmap.


Scoping the Issues
Brainstorm challenges and opportunities in the selected area
Group ideas into themes to form issues
Identify recurring themes and issues within and across WGs
Confirm narrowed scope of issues to be addressed in Roadmap
No
Park other issues to be addressed in later version, or not at all STOP
Gap analysis
Refine description of the Issue Including: keywords + SDOs identification
List any Published Standards
If published standards adequately address the issue, STOP (NO GAP)
List any In-Development Standards
If Yes
State the Gap
Provide a recommendation how to address the gap
Is R&D needed? If so, describe it.
Is the Priority High, Medium, or Low?
List an organization(s) that can address the R&D and standards gap
Use Prioritization Matrix

Understanding the relevance of standards to the data collaborative was a major undertaking, given the breadth of the topic and the magnitude of challenges posed by new technologies along the data supply chain and data governance lifecycle. Consequently, a participatory research methodology was adopted which enabled all working group (WG) members to be involved as subject experts and to bring their perspectives into the knowledge-production process, i.e., the development of the standards roadmap.90

Specifically, each working group followed the following steps to map out the landscape of published standards in accordance with their scope.


Identify Key Themes and Challenges
Prioritize Key Issues
Articulate Issues and Keywords
Search Published Standards
Validate and Triage Standards

[90] Bergold, J., & Thomas, S. (2012). Participatory research methods: A methodological approach in motion. *Historical Social Research/ Historische Sozialforschung*, 191-222.

IDENTIFY KEY THEMES AND CHALLENGES

Members under each WG worked together to brainstorm key themes, challenges, gaps and opportunities under their respective working group scope. Specifically, the following questions were discussed:

- What are social/ technological/ economic/ environmental/ political/ value-related needs?
- What key changes have occurred that pose challenges in these areas?
- Are there any opportunities that we want to pursue but need standardization solutions to facilitate the ability to pursue them?

Results of each brainstorming session were analyzed and grouped into themes to form high-level issues. Subsections of each issue, recurring themes and issues within and across WGs were also identified. In total, 821 notes were captured, which were further categorized into 53 issues.

PRIORITIZE KEY ISSUES

Once the high-level issues were identified, WG members reviewed them together and voted on the level of priority. Specifically, for each issue, members discussed:

- What is the value proposition?
- Do you agree with the proposed scope of the issue?
    - If Agree: Vote on level of priority (high, medium or low); and
      Vote on the working group that should be responsible for leading the issue.
    - If Disagree: Discuss and revise the issue to come to an agreement, then move to vote.

Among the 53 issues that were originally proposed, 10 were merged due to overlap of scopes, six new issues were added and 14 were parked due to lower level of priority or lack of clarity. This resulted in a final list of 35 issues to be included in the standards roadmap.

ARTICULATE ISSUES AND KEYWORDS

Each WG discussed the identified issues assigned to their groups and completed the scoping and description of issues. This included:

- Describing the issue and why it is important from a commercial, civil or public safety perspective;
- Proposing a list of keywords to be used to identify standards associated with the issues/ challenges; and
- Identifying relevant standards development organizations (SDOs) that are applicable to the issue and within the scope of the roadmap.

This led to a list of more than 500 keywords across 35 issues.

SEARCH PUBLISHED STANDARDS

Researchers from SCC took the list of keywords and searched for relevant standards on IHS, a third-party database that provides codes and standards from more than 200 SDOs cross the world.[91] A few criteria were set to identify standards that are most relevant to the DGSC, including:

- Only search for active and latest edition of standards;
- Only search for English and French standards;
- Duplicate standards identified by different keywords but under the same issue were removed, but duplications across different issues were kept since they addressed different topics; and
- Multiple adoptions of the same standards were removed, only keeping the original international standards being adopted.

In total, about 12,000 standards were identified across 35 issues after removing duplications.[92]

VALIDATE AND TRIAGE STANDARDS

The next step of the process was to validate and triage standards identified through the IHS search to remove any irrelevant standards and ensure that relevant standards were not missed. WG members were asked to review and colour-code the list of standards based on the following criteria:

Tier	Description
I	The standard, based on the citation and title, matches not only the keyword but also the description of the issue and looks like its use would address the challenges identified.
II	The standard, based on the citation and title, partially matches either the keyword and/or the description of the issue, where it may either partially address the challenge identified or be useful as a reference in creating a standard to address the challenge identified.
III	The standard, based on the citation and title, would only be useful to the issue in a very limited scope, such as a specific sector or a niche approach.
IV	The standard, based on the citation and title, has no relevance to the issue and the keyword.

Once the review was completed, the triaged results were sent to corresponding SDOs for their input and validation. SDOs were also asked to provide a list of standards under development that may address the 35 issues identified.

[91] IHS Markit. Engineering Workbench: Standards, Codes & Specs. Access at: https://ihsmarkit.com/products/standards-codes-specs.html
[92] Original search of the 500+ keywords generated about 25,000 standards, more than half of which were removed as a result of duplication.

Working groups were then asked to perform the gap analysis evaluation of existing and needed standards, specifications and conformance programs for each issue. A "gap" was defined as meaning that no published standard, specification, etc. exists that covers the particular issue in question. Where gaps were identified and described, working groups included an indication of whether additional pre-standardization R&D is needed, a recommendation for what should be done to fill the gap, the priority for addressing the gap, and an organization(s) – e.g., an SDO or research organization – that potentially could carry out the R&D and/or standards development based on its current scope of activity. Where more than one organization was listed, there was no significance to the order in which the organizations were listed.

Each gap was assessed and ranked using the criteria described below as being high, medium or low priority. In terms of taking action to address the priorities, the desired timeframes are as follows: high priority (0-2 years), medium (2-5 years) and low (5+ years).

Diagram 3: Priority criteria

Criteria (Make the C-A-S-E for the Priority Level)	Scoring Values

Criticality (Safety/Quality Implications) – How important is the project? How urgently is a standard or guidance needed? What would be the consequences if the project were not completed or undertaken? A high score means the project is more critical.	3 – critical;
	2 – somewhat critical;
	1 – not critical

Achievability (Time to Complete) – Does it make sense to do this project now, especially when considered in relation to other projects? Is the project already underway or is it a new project? A high score means there is a good probability of completing the project soon.	3 – project near completion;
	2 – project underway;
	1 – new project

Scope (Investment of Resources) – Will the project require a significant investment of time/work/money? Can it be completed with the information/tools/resources currently available? Is pre-standardization research required? A high score means the project can be completed without a significant additional investment of resources.	3 – low resource requirement;
	2 – medium resource requirement;
	1 – resource intensive

Effect (Return on Investment) – What impact will the completed project have on data governance? A high score means there are significant gains for the industry by completing the project.	3 – high return;
	2 – medium return;
	1 – low return

Score rankings: High Priority (a score of 10-12); Medium Priority (a score of 7-9); Low Priority (a score of 4-6)

This roadmap is supplemented by the DGSC Landscape, a table of standards that are directly or peripherally related to the issues described in the roadmap and can be found in Annex I.

Annex H —

Overview of SDOs and other Entities Operating in the Data Governance Space

SDO Name	Description
American National Standards Committees (ANSI)	ANSI is a private, non-profit organization promoting and facilitating the development of voluntary consensus standards for products, services, processes, systems and personnel, as well as conformity assessment systems in the United States. Among its leadership roles in major global and regional standards and accreditation organizations, ANSI is the sole U.S. representative to ISO and, through the U.S. National Committee, to IEC.
American Society of Civil Engineers (ASCE)	ASCE standards provide technical guidelines for promoting safety, reliability, productivity and efficiency in civil engineering. There are more than 60 published standards.
American Water Works Association (AWWA)	AWWA focuses on publishing consensus standards for equipment and materials used in the treatment and distribution of drinking water in order to build, maintain and operate superior water treatment and distribution systems.
ASTM International (ASTM)	ASTM International, formally the American Society for Testing and Materials, is recognized as a leader in the development and delivery of voluntary consensus standards. ASTM International has published more 12,8000 ASTM standards globally and has more than 140 participating countries.
British Standards Institution (BSI)	BSI is the national standards body of the United Kingdom. It is a non-profit distributing organization and offers global services in the linked fields of standardization, system assessment, product certification, training and advisory services. BSI produces technical standards on a wide range of products and services and also supplies certification and standards-related services to businesses.
CIO Strategy Council (CIOSC)	CIOSC is a Canadian standards development organization, accredited by SCC. Its primary focus is the development of standards in emerging technologies within Canada's information and communications technology (ICT) sector. CIOSC has published standards on data governance, digital trust and identity, and artificial intelligence. Current notable working groups include: • TC 1: Data Governance • TC 4: Digital Trust and Identity • TC 10: Open Banking
Clinical and Laboratory Standards Institute (CLSI)	CLSI is a U.S.-based non-profit organization that develops and publishes consensus standards for the healthcare industry. It has a membership of more than 1,400 organizations and 400 individuals from 60 countries. CLSI is active in ISO and serves as the secretariat of ISO/TC 212: the technical committee for clinical laboratory testing and in-vitro diagnostic test systems.

CSA Group (CSA)	CSA is a Canadian standards development organization, accredited by SCC. It is one of the largest standards development organizations in North America and has offices in Europe, and Asia. CSA's standardization activities have a wide focus, including areas such as construction, energy, health, ICT and transportation. CSA has published the Canadian adoptions of a large number of ISO standards, related to IT, cybersecurity, among others.
Danish Standards Foundation (DS)	DS is a private, independent, non-governmental organization and serves as the national standardization organization of Denmark. DS offers standardization services in a variety of areas, ranging from the development of standards to the sale of standards and related publications. DS is a member of the ISO, IEC, CEN, CENELEC and ETSI.
Decentralized Identity Foundation (DIF)	DIF is an industry group promoting enablement of decentralized identity solutions so that entities gain control over their identities and trusted interactions can occur. It supports industry-wide discussions and contributions to open source code, and supports interoperability. Its ongoing projects include work on Universal Resolver, Universal Registrar, Peer DID Method Specification, among others. The foundation consists mostly of American leadership but includes global participation. Its members include Microsoft, Hyperledger, Accenture, SecureKey, and the British Columbia Ministry of Citizens' Services.
Digital ID and Authentication Council of Canada (DIACC)	DIACC is a Canadian non-profit coalition of private and public organizations, looking to develop a Canadian framework for digital identification and authentication. It has published the Pan-Canadian Trust Framework (PCTF), a set of digital identity and authentication standards, to help businesses and governments develop tools and services while promoting interoperability, user-centric design, privacy, security and convenience. DIACC has three committees, including the Trust Framework Expert Committee, which delivered the PCTF and develops standards and supporting materials to secure identity service interoperability. DIACC helped found the Digital Identity Laboratory of Canada, which offers evaluation, testing and certification services for digital identity solutions regarding their compliance and interoperability.
European Telecommunications StandardS Institute (ETSI), **European Committee for Electrotechnical Standardization (CENELEC),** **European Committee for Standardization (CEN)**	ETSI, CENELEC and CEN are the three bodies officially recognized by the European Union as a European Standards Organization (ESO). ETSI is the officially recognized standardization representative for ICT, telecommunications, broadcasting and other electronic communication networks, CENELEC is for electrical and electrotechnical engineering, and CEN is for all other technical areas. Two relevant technical committees are jointly under CEN and CENELEC, and one relevant technical committee under CEN: • CEN/CLC/JTC 13 – Cybersecurity and Data Protection • CEN/CLC/JTC 19 – Blockchain and DLT • CEN/TC 224 – Personal identification and related personal devices with secure element, systems, operations and privacy in a multi-sectorial environment Of note are the ISO/IEC 27000 series of standards, which relate to information security management. A number of these standards were originally published by CEN/CENELEC and have been adopted by ISO.
FIDO Alliance	The FIDO Alliance is an open industry association with a focus on authentication standards to help reduce the world's over-reliance on passwords. It promotes the development of, use of, and compliance with standards for authentication and device attestation. Its membership includes several large multinationals, including Amazon, American Express, Apple, Bank of America, Facebook, Google, Intel, Microsoft, Qualcomm, Samsung, Visa and Wells Fargo, among others.

Financial Data Exchange (FDX)	FDX is an American non-profit organization that promotes the broad adoption of a common, interoperable and royalty-free standard for the secure access of user-permissioned financial data, named the FDX API. FDX has an international membership that promotes user-permissioned data sharing principles and includes financial institutions, financial data aggregators, fintechs, payment networks, consumer groups, financial industry groups and utilities, and other permissioned parties in the user-permissioned financial data ecosystem. While it is based in the U.S., FDX recently launched a Canadian Working Group. This group includes 31 Canadian financial industry organizations, including BMO, CIBC, Desjardins, EQ Bank, Flinks, Interac, Intuit, Mastercard, National Bank, RBC, Scotiabank, SecureKey and TD, among others. The Canadian Working Group is represented on the FDX Board by RBC and Interac (Interac is a cooperative venture launched in 1984 by RBC, CIBC, Scotiabank, TD, and Desjardins).
German Institute for Standardization (DIN)	DIN is the German national organization for standardization and is the German ISO member body. DIN develops norms and standards for rationalization, quality assurance, environmental protection, safety and communication in various fields such as technology, science, industry, government and the public domain.
Hyperledger	Hyperledger is an open-source community focused on developing a suite of stable frameworks, tools and libraries for enterprise-grade blockchain deployments. It is a global collaboration, hosted by The Linux Foundation, and includes leaders in finance, banking, Internet of Things, supply chains, manufacturing and technology. Members include IBM, Hitachi, JPMorgan, American Express, Digital Asset (DAML), FedEx, Huawei, Lenovo, R3, Red Hat, Ripple, SAP, SecureKey, Walmart, and others. Associate members include Bank of England, Decentralized Identity Foundation, GS1, Government of British Columbia, Sovrin Foundation, Yale University, and others. This initiative has various open-source projects, most notably: • Aries – Infrastructure for blockchain-rooted, peer-to-peer interactions. It provides a shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting and storing verifiable digital credentials. • Indy – Distributed ledger purpose-built for decentralized identity. • Ursa – A shared cryptographic library that enables people (and projects) to avoid duplicating cryptographic work across projects, increasing security in the process.
Institute of Electrical and Electronics Engineers (IEEE)	IEEE is a professional association for electronic and electrical engineering and related disciplines. It also has a standard setting body for a broad range of fields related to engineering and computer science. IEEE is organized into various communities, societies, technical councils, technical communities and working groups, based on subject matter and areas of expertise.
International Commission on Illumination (CIE)	CIE is an organization devoted to international cooperation and exchange of information among its member countries on matters concerning the science and art of lighting. Regarded as the international authority on light, illumination colour, and colour spaces, CIE publishes standards guiding the science and art of light and lighting, colour and vision, photobiology and image technology.
International Electrotechnical Commission (IEC)	The International Electrotechnical Commission is an international standards organization that prepares and publishes international standards for all electrical, electronic and related technologies. IEC has many joint technical committees with ISO, most notably ISO/IEC JTC 1.

International Organization for Standardization (ISO)	ISO is the largest independent, non-governmental, international SDO, with a membership of 165 national standards bodies. ISO brings together experts to develop voluntary, consensus-based standards. ISO has been active in the development of various information technology standards, mainly spearheaded by one technical committee, ISO/IEC JTC 1 Information Technology and several of its subcommittees, primarily: • ISO/IEC JTC 1/SC 17 – IT – Cards and security devices for personal identification; • ISO/IEC JTC 1/SC 27 – IT – Information security, cybersecurity, and privacy protection; • ISO/IEC JTC 1/SC 31 – IT – Automatic identification and data capture techniques; • ISO/IEC JTC 1/SC 32 – IT – Data management and interchange.
International Telecommunication Union – Telecommunication Standardization Sector (ITU-T)	ITU-T is one of the three sectors of the International Telecommunication Union (ITU), a specialized agency of the United Nations for information and communication technologies (ICT). ITU-T coordinates standards for telecommunications and ICT and has a number of study groups and focus groups within its structure. Of note is Study Group 17: Security and Focus Group on Application of DLT.
International Telecommunication Union – radiocomunication Sector – Recommendations (ITU-R)	ITU-R Recommendations constitute a set of international standards developed by the Radiocommunication Sector of the ITU. ITU-R Recommendations are approved by ITU Member States and are developed by experts from administrations, operators, the industry and other organizations dealing with radiocommunication matters globally.
Internet Engineering Task Force (IETF)	IETF is an open standards organization, referred to by some as the 'leading internet standards body.' IETF develops voluntary internet standards, notably the standards comprising the Internet Protocol Suite (TCP/IP). Within its structure it includes the OAuth Working Group, which developed the OAuth Protocol.
Internet Society	The Internet Society is an American-based non-profit organization with participants from around the world that works to 'grow and strengthen the Internet.' It supports internet accessibility, advances the development and application of internet infrastructure, technologies, and open standards, and provides leadership in internet policy. The organization promotes a decentralized approach to how the internet works and collaborates with like-minded organizations around the world. It facilitates open development of standards and protocols, supports education in developing countries, and promotes professional development and forums for discussion of issues, etc. Its membership includes companies such as Comcast, Amazon, AT&T, Google, Mozilla, CERN, Facebook, LinkedIn, Nokia and Tencent, among others.
Kantara Initiative	Kantara is an American-based non-profit industry professional trade association that offers service providers third-party conformity assessment and assurance approval against its NIST 800-63-3 Class of Approval under its Identity Assurance Trust Framework. It also develops specifications and submits them to formal standardization bodies to fill emerging industry and marketplace needs. Its membership is comprised of companies from North America, Europe and Oceania, including Experian, Idemia, digi.me, Identos, and Mastercard. It also has liaisons or partner agreements with organizations such as DID Alliance, Digital Identity New Zealand, Financial Data Exchange, FIDO Alliance, European Association for e-Identity and Security, and the Digital Identity and Authentication Council of Canada (DIACC), among others.

National Fire Protection Association (NFPA)	NFPA develops, publishes and disseminates more than 300 consensus codes and standards intended to minimize the possibility and effects of fire and other risks.
National Institute of Standards and Technology (NIST)	NIST is a laboratory and non-regulatory agency of the United States Department of Commerce. Its activities are organized into laboratory programs that include nanoscale science and technology, engineering, information technology, neutron research, material measurement and physical measurement.
OASIS Open	OASIS is a non-profit standards body working to advance the fair, transparent development of open source software and standards through the power of global collaboration and community. People join OASIS to advance projects for cybersecurity, blockchain, IoT, emergency management, cloud computing, legal data exchange, and much more. It also participates in global standards development in ISO, through the American standardization body, ANSI. It is active in ISO/PC 317 (Privacy by Design for Consumer Goods and Services) and ISO/TC 324 (Sharing Economy). Its foundation sponsor is IBM, and it also has a long list of other sponsors and contributors, including Adobe, Cisco, Dell, HP, Huawei, McAfee, Microsoft, Red Hat, TELUS, US Department of Defense, Bank of America, Ethereum Foundation, Google and Boeing, among others.
Open Banking Initiative Canada (OBIC)	OBIC is an organization that represents the financial services industry (consumers, fintechs, banks and industry experts) working to initiate and lead the development of an open banking framework in Canada. The ecosystem it is developing will evaluate technology and standards that are intended to foster a trust framework between fintechs, banks and regulatory bodies within Canada. OBIC's Board includes representation from Wealthsimple, Axway, The AML Shop, the Large Credit Union Coalition and the Canadian Credit Union Association.
OpenID Foundation (OIDF)	OIDF is a non-profit international standardization organization of individuals and companies committed to enabling, promoting and protecting OpenID technologies. It serves as a public trust organization representing the community of developers, vendors and users, and assists the community by providing needed infrastructure and help in promoting and supporting expanded adoption of OpenID. OIDF published Open ID Connect 1.0 as an identity layer on top of the OAuth 2.0 protocol. It enables clients to verify the identity of the end-user based on the authentication performed by an authorization server, and to obtain basic profile information about the end-user. There are various working groups within the OIDF, including: • Enhanced Authentication Profile (EAP) WG • eKYC and Identity Assurance (eKYC & IDA) WG • International Government Assurance Profile (iGov) WG Its sponsoring members include Google, Microsoft,and Verizon, while other members include Amazon Web Services (AWS), Deutsche Telekom, eBay, Intuit and Paypal, among many others.
SAE International (SAE)	SAE is a U.S.-based standards developing organization for engineering professionals. Standards from SAE are used to advance mobility engineering globally. The SAE Technical Standards Development Program is among the organization's primary provisions to those mobility industries it serves: aerospace, automotive, and commercial vehicle.
Standards New Zealand (SNZ)	SNZ is the national standards body for New Zealand and is a business unit within the Ministry of Business, Innovation and Employment. SNZ specializes in managing the development of standards and publishes and sells New Zealand, joint Australian-New Zealand, and international standards.

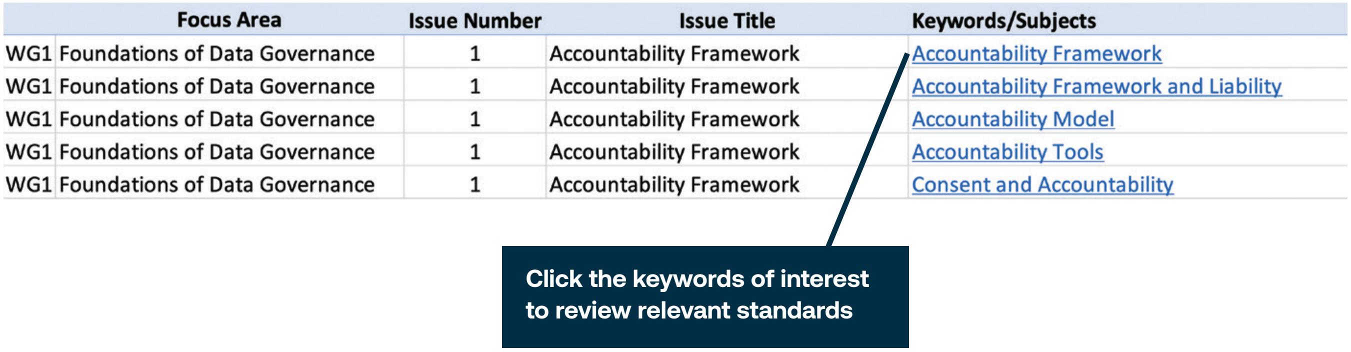
Canadian General Standards Board (CGSB)	CGSB is a federal government organization that offers client-centred, comprehensive standards development and conformity assessment services in support of the economic, regulatory, procurement, health, safety and environmental interests of its stakeholders. CGSB is accredited by SCC as a SDO and is also accredited as a product certification body and a management systems certification body.
The First Nations Information Governance Centre (FNIGC)	The First Nations Information Governance Centre is an independent, apolitical and technical non-profit organization operating with a special mandate from the Assembly of First Nations' Chiefs-in-Assembly (Resolution #48, December 2009). FNIGC is committed to providing quality information that contributes to improving the health and well-being of First Nations people in Canada. In collaboration with its regional partners, FNIGC conducts unique data-gathering initiatives that enable its partners to support First Nations governments to build culturally relevant portraits of their communities. FNIGC supports First Nations communities by contributing directly to building data and statistical capacities at national, regional and community levels, including the provision of credible and relevant information on First Nations. In addition to conducting a number of surveys, FNIGC is responsible for a wide range of other work. It oversees data collection on First Nations reserves and in northern communities, conducts research, engages in knowledge translation and dissemination activities, offers education and training, and promotes the advancement of the First Nations principles of OCAP®. Critically, FNIGC and its regional partners follow established protocols, policies and procedures that are guided by a holistic cultural framework. Ultimately, FNIGC is a tool that rights-holding First Nations can use, via their governance, to assert sovereignty over their data and information. The First Nations principles of OCAP® establish how First Nations' data and information will be collected, protected, used or shared. OCAP® is a tool to support strong information governance on the path to First Nations data sovereignty.
National Electrical Manufacturers Association (NEMA)	NEMA is an ANSI-accredited standards development organization comprised of business leaders, electrical experts, engineers, scientists and technicians. NEMA publishes more than 700 electrical and medical imaging standards and technical whitepapers covering millions of Member products.
Underwriters Laboratories of Canada (ULC)	ULC standards is accredited by SCC as a consensus-based SDO under the National Standards System of Canada. ULC develops and publishes standards as well as specifications for products concerning fire, life safety and security, crime prevention, energy efficiency, environmental safety, security of assets and facilities, live working and workplace safety.
World Wide Web Consortium (W3C)	W3C is one of the main international standards organizations for the World Wide Web. W3C has several working groups working on standards related to digital identity, credentials and authentication: • Verifiable Credentials Working Group • Decentralized Identifier (DID) Working Group • Web Application Security Working Group • Web Authentication Working Group W3C also has several community groups that publish reports but do not write standards: • Credentials Community Group • Digital Identity Community Group • Digital Verification Community Group • User Identity on the Web Community Group

Annex I —

The DGSC Standardization Landscape

INSTRUCTIONS ON HOW TO REVIEW STANDARDS LANDSCAPE (click here to download the Excel File)

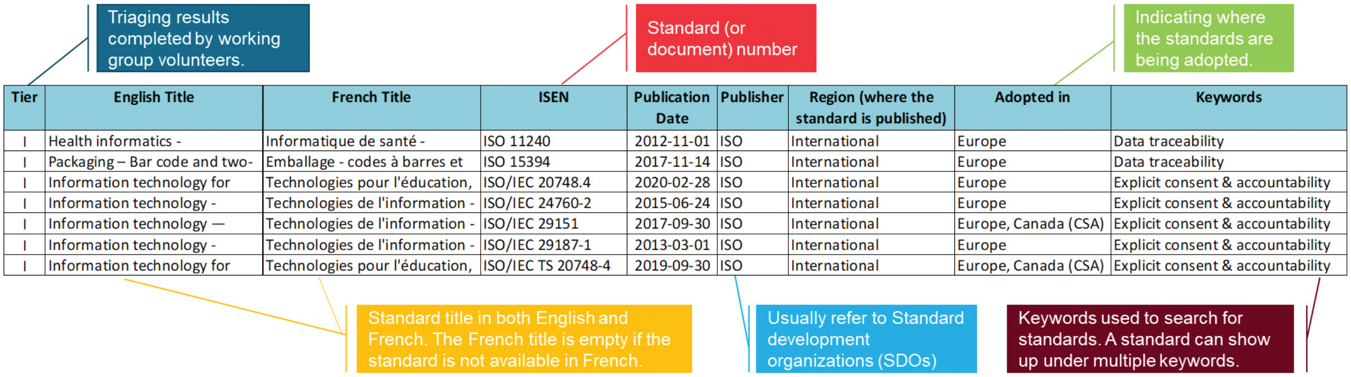
The Index page provides a summary of all keywords under the 35 Issues identified:
Clicking Keywords/Subjects will bring you to the sheet where standards related to the keyword are listed.



Focus Area		Issue Number	Issue Title	Keywords/Subjects
WG1	Foundations of Data Governance	1	Accountability Framework	Accountability Framework
WG1	Foundations of Data Governance	1	Accountability Framework	Accountability Framework and Liability
WG1	Foundations of Data Governance	1	Accountability Framework	Accountability Model
WG1	Foundations of Data Governance	1	Accountability Framework	Accountability Tools
WG1	Foundations of Data Governance	1	Accountability Framework	Consent and Accountability

Click the keywords of interest to review relevant standards

The other 35 sheets contain standards found that are related to each Issue (one sheet per Issue). Below is a quick overview of the structure (title row) in the Issue sheet.



Triaging results completed by working group volunteers.

Standard (or document) number

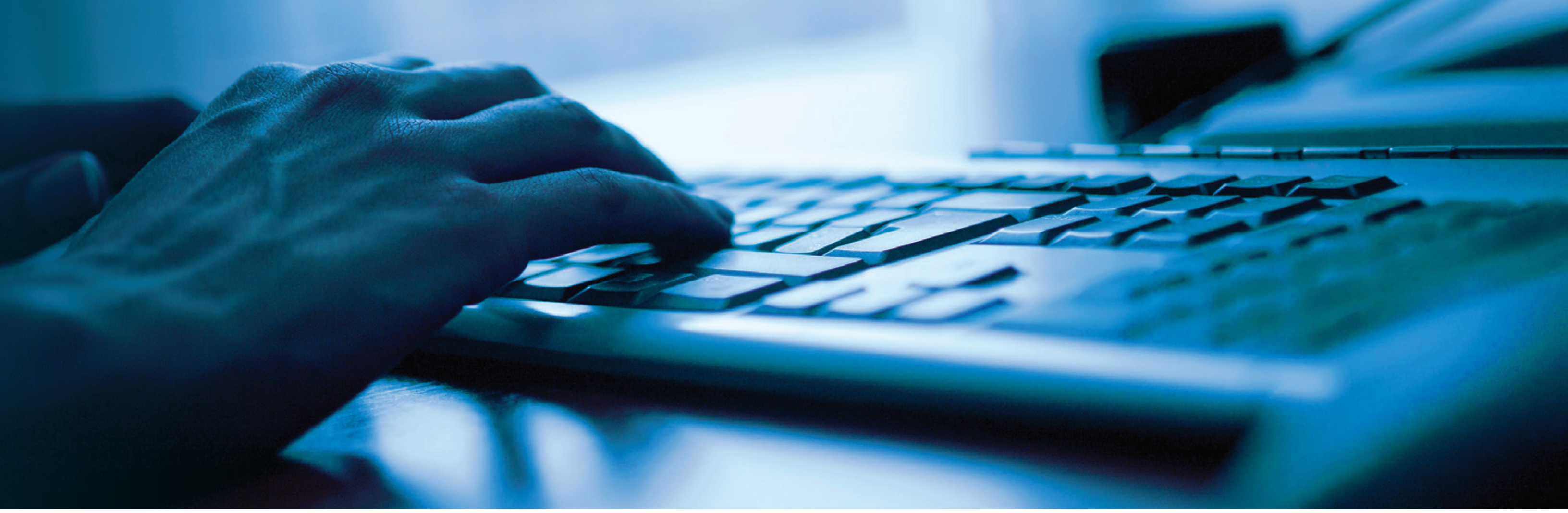
Indicating where the standards are being adopted.

Tier	English Title	French Title	ISEN	Publication Date	Publisher	Region (where the standard is published)	Adopted in	Keywords
I	Health informatics -	Informatique de santé -	ISO 11240	2012-11-01	ISO	International	Europe	Data traceability
I	Packaging – Bar code and two-	Emballage - codes à barres et	ISO 15394	2017-11-14	ISO	International	Europe	Data traceability
I	Information technology for	Technologies pour l'éducation,	ISO/IEC 20748.4	2020-02-28	ISO	International	Europe	Explicit consent & accountability
I	Information technology -	Technologies de l'information -	ISO/IEC 24760-2	2015-06-24	ISO	International	Europe	Explicit consent & accountability
I	Information technology —	Technologies de l'information -	ISO/IEC 29151	2017-09-30	ISO	International	Europe, Canada (CSA)	Explicit consent & accountability
I	Information technology -	Technologies de l'information -	ISO/IEC 29187-1	2013-03-01	ISO	International	Europe	Explicit consent & accountability
I	Information technology for	Technologies pour l'éducation,	ISO/IEC TS 20748-4	2019-09-30	ISO	International	Europe, Canada (CSA)	Explicit consent & accountability

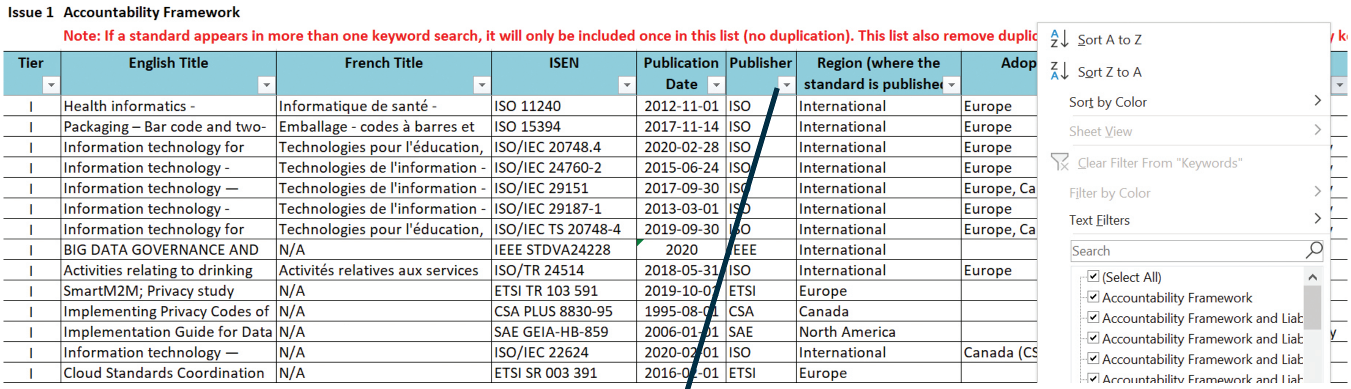
Standard title in both English and French. The French title is empty if the standard is not available in French.

Usually refer to Standard development organizations (SDOs)

Keywords used to search for standards. A standard can show up under multiple keywords.



To review standards under specific Issues, you can filter by Title, ISEN (standard number), publisher (i.e., the standard development organizations) or by keywords. Please use the Filter function in Excel to filter areas of interest and search for standards that you would like to review.



Issue 1 Accountability Framework

Note: If a standard appears in more than one keyword search, it will only be included once in this list (no duplication). This list also remove duplic

Tier	English Title	French Title	ISEN	Publication Date	Publisher	Region (where the standard is publishe	Adop
I	Health informatics -	Informatique de santé -	ISO 11240	2012-11-01	ISO	International	Europe
I	Packaging – Bar code and two-	Emballage - codes à barres et	ISO 15394	2017-11-14	ISO	International	Europe
I	Information technology for	Technologies pour l'éducation,	ISO/IEC 20748.4	2020-02-28	ISO	International	Europe
I	Information technology -	Technologies de l'information -	ISO/IEC 24760-2	2015-06-24	ISO	International	Europe
I	Information technology —	Technologies de l'information -	ISO/IEC 29151	2017-09-30	ISO	International	Europe, Ca
I	Information technology -	Technologies de l'information -	ISO/IEC 29187-1	2013-03-01	ISO	International	Europe
I	Information technology for	Technologies pour l'éducation,	ISO/IEC TS 20748-4	2019-09-30	ISO	International	Europe, Ca
I	BIG DATA GOVERNANCE AND	N/A	IEEE STDVA24228	2020	IEEE	International	
I	Activities relating to drinking	Activités relatives aux services	ISO/TR 24514	2018-05-31	ISO	International	Europe
I	SmartM2M; Privacy study	N/A	ETSI TR 103 591	2019-10-01	ETSI	Europe	
I	Implementing Privacy Codes of	N/A	CSA PLUS 8830-95	1995-08-01	CSA	Canada	
I	Implementation Guide for Data	N/A	SAE GEIA-HB-859	2006-01-01	SAE	North America	
I	Information technology —	N/A	ISO/IEC 22624	2020-02-01	ISO	International	Canada (CS
I	Cloud Standards Coordination	N/A	ETSI SR 003 391	2016-02-01	ETSI	Europe	

Sort A to Z
Sort Z to A
Sort by Color
Sheet View
Clear Filter From "Keywords"
Filter by Color
Text Filters
Search
☑ (Select All)
☑ Accountability Framework
☑ Accountability Framework and Liab
☑ Accountability Framework and Liab
☑ Accountability Framework and Liab
☑ Accountability Framework and Liab

Filter by areas of interest and search for standards that you would like to review.