Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

The Canadian Cyber Security Skills Framework

Adapting the NICE Framework for the Canadian labour market

Management

Canada

Foreword

The Canadian Cyber Security Skills Framework (ITSM.00.039) is an unclassified publication that has been issued under the authority of the Head of the Canadian Centre for Cyber Security (Cyber Centre). For more information, email or phone our Service Coordination Centre:

Contact Centre
contact@cyber.gc.ca
(613) 949-7048 or 1-833-CYBER-88

Due to the highly dynamic nature of cyber security, this guide will be reviewed annually by the Canadian Centre for Cyber Security's Academic Outreach and Engagement Team. All proposed changes to this publication should be sent by email to:

academicoutreach-collaborationacademique@cyber.gc.ca.

Effective date

This publication takes effect on April 19, 2023.

Revision history

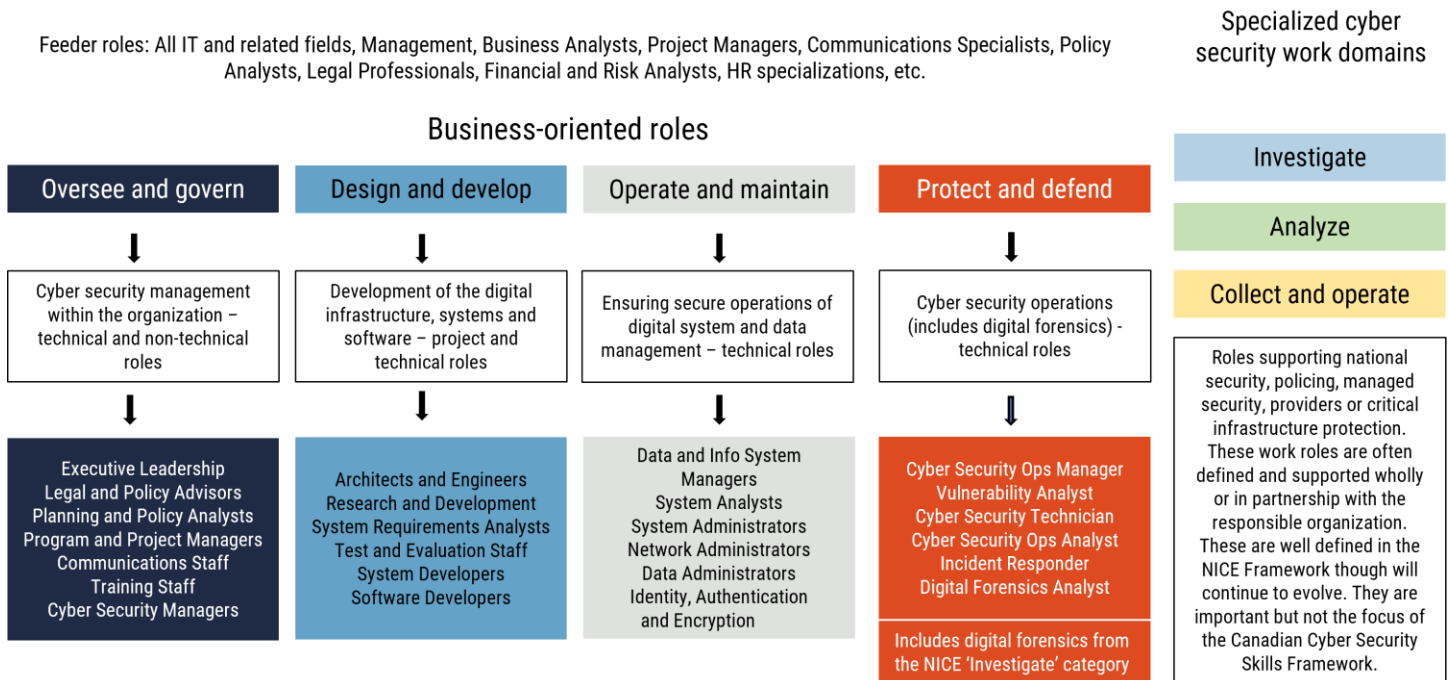| Revision	Amendments	Date
1	First release.	April 19, 2023

Overview

The Canadian Cyber Security Skills Framework (Figure 1) is based on elements of the U.S. NICE [Workforce Framework for Cybersecurity](#) (NICE framework), contextualized for the Canadian labour market. It's a model that leverages the NICE framework while simplifying it using a business-oriented lens recognizing talent from an organizational security perspective and is a model more accessible to non-cyber security stakeholders.

Figure 1: Canadian Cyber Security Skills Framework

Feeder roles: All IT and related fields, Management, Business Analysts, Project Managers, Communications Specialists, Policy Analysts, Legal Professionals, Financial and Risk Analysts, HR specializations, etc.

Specialized cyber security work domains

Business-oriented roles

Oversee and govern	Design and develop	Operate and maintain	Protect and defend
Cyber security management within the organization – technical and non-technical roles	Development of the digital infrastructure, systems and software – project and technical roles	Ensuring secure operations of digital system and data management – technical roles	Cyber security operations (includes digital forensics) - technical roles
Executive Leadership Legal and Policy Advisors Planning and Policy Analysts Program and Project Managers Communications Staff Training Staff Cyber Security Managers	Architects and Engineers Research and Development System Requirements Analysts Test and Evaluation Staff System Developers Software Developers	Data and Info System Managers System Analysts System Administrators Network Administrators Data Administrators Identity, Authentication and Encryption	Cyber Security Ops Manager Vulnerability Analyst Cyber Security Technician Cyber Security Ops Analyst Incident Responder Digital Forensics Analyst Includes digital forensics from the NICE 'Investigate' category

Investigate

Analyze

Collect and operate

Roles supporting national security, policing, managed security, providers or critical infrastructure protection. These work roles are often defined and supported wholly or in partnership with the responsible organization. These are well defined in the NICE Framework though will continue to evolve. They are important but not the focus of the Canadian Cyber Security Skills Framework.

Leveraging the core elements and characteristics of the NICE framework, the Canadian Cyber Security Skills Framework will:

- help to specify the cyber security workforce gaps that exist in the Canadian labour market by applying a business lens and distinguishing between core cyber security roles and organizational roles which have some cyber security responsibilities or cyber security adjacent roles

- simplify the representation of cyber security-related work that is common within most organizations

- adapt to support broader or generalist responsibilities common within small and medium organizations (SMOs) as they aim to address foundational information technology (IT) and cyber security requirements

- maintain emphasis on cyber security responsibilities of adjacent work roles within "oversee & govern", "design & develop", and "operate & maintain"

The Canadian Cyber Security Skills Framework is a simpler presentation of cyber security work represented within many private and smaller public sector organizations. The purpose of this framework is to help better guide workforce development stakeholders in addressing the cyber security skills deficit. It can be applied across public, private, and academic sectors for career awareness and development, education and training, recruitment, or workforce planning.

Table of contents

List of figures

List of tables

List of annexes

1 Applying the NICE framework in Canada

1.1 Background

The National Occupational Standard (NOS) defines primary cyber security work as distinct from other occupations in IT, security, business management, or public administration. Cyber security is not, however, just about technical systems. It's also about people, their behaviour, and how they connect and engage with these systems.

The value of effective cyber security, and the services and products supported by cyber security professionals, cannot be understated. Cyber security work is now known across the globe as a critical and enduring career within the digital economy.

In Canada, our reliance on information and data systems has increased exponentially over the past decade as organizations digitize their operations and move to an online presence. This requires professionals who can design, build, implement, and maintain safe, secure, and reliable information systems that can support a variety of business, operational, and personal needs.

Canadian citizens have become more aware of their privacy rights and are increasingly concerned about how their personal data is protected by organizations. This requires experts in both online security and privacy who can advise on the various national and international standards, develop policies, identify requirements, and support monitoring to better protect the privacy of Canadians.

Cybercrime is an ever-increasing threat. According to the Cyber Centre's National Cyber Treat Assessment 2020, "cyber threat actors pose a threat to the Canadian economy by exacting costs on individuals and organizations, notably through the theft of intellectual property and proprietary information" [1]. Expertise is required to support detection and response to cyber threats as well as to support those who will investigate and collect digital evidence that can be used in improving protections and, when required, prosecuting offenders.

Cyber security will continue to be required across a broad range of technologies. Those employed in this field have significant and lasting career opportunities that can positively affect the lives of connected Canadians and support the future of the digital economy.

Consequently, Canadian businesses and industries struggle to meet their cyber security needs. There are four key workforce development challenges:

- Generating and retaining cyber security operations talent to meet the needs of the Canadian labour market
- Ensuring contributing technical and non-technical roles have required knowledge, skills, and abilities (KSAs)
- Being responsive to the changing technology landscape
- Normalizing cyber security work and activities within the Canadian workplace

In part to help address these challenges, a group of industry, government, and academic stakeholders formed the Cyber Talent Alliance (see Annex F – available upon request). The group worked together to deliver:

- A cyber security skills framework, including taxonomy and common lexicon that describes cyber security work and workers, based on elements of the U.S. NICE framework[1] contextualized for the Canadian labour market

- NOS descriptions based on the skills framework

- Learning outcomes for relevant workforce areas

- Related resources to support workforce, career development, and learning

---

[1] The NICE Workforce Framework for Cyber Security, formerly the NICE Cyber Security Workforce Framework, was re-named in 2020 to recognize that cyber security is a concern across all workforces, not just the cyber security workforce.

2 A brief introduction to the NICE framework

Before the NICE framework, the diversity of ways in which cyber security work was viewed and described within the U.S. federal government posed a significant problem with recruiting, selection, training, and other workforce development activities across both the public and private sectors. Given the increasing threats to both the national and economic security, this was untenable. While conceived in the late 2000s, the first NICE working group was formed in 2011 by the U.S. National Institute of Standards and Technology (NIST) with other U.S. federal partners. Since then, over 20 U.S. federal departments, defence and security industry stakeholders, academia, and limited international participation from allies, such as Canada and Australia have contributed to the development and the evolution of the NICE framework.

The NICE framework provides an integrated view of the cyber security workforce. This means that it identifies work roles that "have an impact on an organization's ability to protect its data, systems, and operations" [2]. This includes both technical and non-technical roles intended to support organizational cyber security risk management efforts. In addition, the NICE framework includes national cyber operations capabilities including intelligence and offensive operations work roles normally housed within the federal government or partner institutions. Notably, the NICE framework includes an oversight and revision process to ensure that it meets the evolving needs of the cyber security community.

2.1   The U.S. NICE framework in the Canadian context

The NICE framework provides a comprehensive account of cyber security work. The degree to which it can be readily adopted by Canadian business and industrial organizations was a central point of investigation within this project. A few key questions are addressed:

1. **What are the key issues associated with the Canadian cyber security workforce?**

There are several issues when exploring differences and similarities between the U.S. and Canadian cyber security labour market.

Similarities:

- Both countries experience a lack of labour market information on cyber security jobs, related job titles, and roles.
- Based on the NICE framework work roles, Canada is assessed as having a similar gap as the U.S.
- In Canada, there are fewer resources dedicated to and limited attention on the cyber security workforce challenge.
- Cyber security is a highly competitive employment environment in both countries.

Differences:

- Canada and the U.S. have similar job market, but Canada has a considerably smaller and more dispersed work population.
- Resources are required in both official languages in Canada.
- A larger portion of Canada's economy is comprised of small and medium organizations (SMOs) and their needs differ from larger organizations.

- Canadian businesses and industries have limited visibility of the NICE framework and how it may apply to the Canadian labour market.

2. Is the NICE framework open for adoption?

As indicated in the NICE framework, it can be leveraged by other nations and adapted to suit their context [3]. Beyond this, there is also a long history of Five Eyes nations[2] sharing their publications and processes with partners. Canada shares its work with the U.S. and many of the Canadian federal IT security guidance publications are based on or significantly draw on NIST publications.[3]

3. What are the advantages and disadvantages of adopting the NICE framework in its current form?

Advantages:

- Can easily be accessed by the Canadian labour market and workforce development stakeholders
- Standardizes cyber security work role descriptions and provides a common lexicon for the community within the U.S. and Canada as well as other nations
- Provides a detailed description of KSAs for common cyber security roles, and recently introduced associated competencies that will aid in training, education, and career development
- Creates a known baseline to assess skilled entry candidates
- Is supported internationally by other governments
- Supports worker portability nationally and internationally
- Outlines many work roles, tasks, and KSAs that are valid within the Canadian cyber security workforce

Disadvantages:

- Lacks specificity and accuracy on the actual workforce gap to be addressed
- Is too "big" and too granular for the general Canadian market
- Can be difficult to navigate (e.g. the use of codes to cross-references KSAs versus word descriptions)
- Is "defence industry-oriented" or suited to large organizations which are heavily engaged in online activity
- Is structured with a static/horizontal perspective as it's difficult to see career pathways, lateral or vertical progression within the cyber security work domain
- Does not scale well to smaller organizations
- Disregards cyber security generalist functions (e.g. corporate security officer) or those who support multiple cyber security roles within a typical organizational context (common in non-technical small and medium organizations)
- Minimizes important and distinct roles by incorporating them within broader roles (e.g. security engineering is part of the research and development role).

---

2 The Five Eyes is an informal title of the international intelligence sharing agreement between Canada, the U.S., the U.K., Australia and New Zealand.
3 For examples, see https://www.cyber.gc.ca/en/publications.

- Omits operational and industrial technology security roles (e.g. industrial control systems (ICS) and supervisor control and data acquisition (SCADA))
- Overlooks new and emerging roles that respond to the dynamic field of cyber security

The NICE framework does not necessarily reflect structure and employment functions that are common within the Canadian private sector or non-federal public sector organizations.

While there are several other contributing or adjacent cyber security roles noted in the NICE framework, the Canadian framework focuses on core cyber security roles and related competencies that are situated within the broader Canadian business context where most of their work is tied to organizational cyber security objectives and outcomes. Cyber security specializations that are almost solely within the intelligence, national security, or policing domain are identified and detailed within the NICE framework.

2.2 A special note on educators

The valuable role that educators play in cyber security is noted. However, as educators have their own National Occupation Classification (NOC) and an extensive network of occupational and professional standards, there is no need to reiterate that information within this publication. It's recognized that qualified educators are required who have relevant experience and the ability to facilitate and assess required learning to support industry demand according to recognized standards.

2.3 National Occupational Standards (NOS)

National Occupational Standards (NOS) describe what an individual in a particular occupation must know and be able to do to be considered "capable" in the occupation. These standards are defined in terms of competencies, including KSAs required to do the related work effectively, safely, and properly. NOS provide the benchmark for competent performance in the workplace as agreed to by a representative sample of workers, employers, and other stakeholders. NOS may also include or be driven by other external requirements, such as legal or policy compliance.

Figure 2: NOS uses

Practitioners	Employers	Educators	Workforce development stakeholders
Providing a foundation for career development Guiding their learning and development within the occupation Supporting career mobility and transitions	Identifying key tasks and roles Identifying professional development needs Facilitating objective job descriptions Providing guidance for recruitment	Identifying areas where expertise is required Providing the basis for curriculum, training development and education - private and public sector providers Providing curriculum improvements Forming the basis for certification programs and program accreditation	Creating professional development opportunities Identifying the skills required for specific occupations Providing nationally-recognized, sector-driven benchmarks of best practices Providing career development information for practitioners laddering to administration

3 Adapting the NICE framework to the Canadian labour market

3.1   Attributes of a workable skills framework for the Canadian market

By adopting and simplifying the NICE framework for the Canadian labour market and simplifying it, the Canadian framework can be more easily used by businesses and industries who may struggle with interpreting the NICE framework in its original form.

As shown in Figure 3, five key attributes have been identified to be considered when adopting the NICE framework for Canadian use. These attributes were determined based on some criticisms and structural issues of the NICE framework as well as community feedback and consultations.

Figure 3: Desired attributes for the Canadian cyber security skills framework

Specificity and accuracy — While the NICE framework describes the full spectrum of cyber security work roles, there should be a means of focusing on those that are most relevant to addressing the Canadian cyber security skills gap and the Canadian context.

Usability and accessibility — Any framework should allow for ease of use, readability, and accessibility of the content for all potential readers and users. This includes those unfamiliar with cyber security work. More specifically, the framework should not "silo" cyber security, but rather integrate concepts into the broader business/organizational context.

Clarity in constructs — Clarity is required in the constructs used to define cyber security roles and should include not only specialist roles, but generalists, non-technical and cross-disciplinary roles.

Adaptability — To address this dynamic field, there should be a means to rapidly integrate new or emerging roles as a result of technologies such as automation, cloud, artificial intelligence (AI), quantum. Related competencies/KSAs should also be developed to support the breadth of cyber security activities. The framework should be constantly evolving with the work.

Scalability — Any framework should be able to be readily scaled from large to small and medium organizations and different industry contexts. This includes the ability of organizations to identify and develop non-technical talent to support their security needs.

3.2   Adapting the Canadian framework to small and medium organizations

The Canadian framework can be adapted to SMOs. Within cyber security, most SMOs have the following characteristics:

- Lack of in-house cyber security expertise
- "Design & develop" roles are either outsourced or systems and applications are acquired "off-the-shelf"
- Individuals will often fill multiple roles that include cyber security tasks

Consequently, when organizations look at the NICE framework it may be overwhelming. However, there is the potential to identify scenarios or present examples that will help SMOs scale the NICE framework using the Canadian framework. This will also help define role-based KSAs that will support cyber security within organizations.

The following section reviews two common scenarios typically found within SMOs.

1. **Medium-sized organization with some in-house IT staff**

There remains technical expertise in-house, but several cyber security roles are assumed by those who have other functions. They are not typically cyber security specialists or may have only a small IT section who will be responsible for detection and incident response. In this example, the chief information officer (CIO) would lead the small IT team and assume responsibilities for the technical aspects of the cyber security program while the executive level managers would remain responsible for defining the business priorities and risk landscape. For all "protect & defend" functions, they would likely be assumed by the IT team with specialized activities outsourced to a third party.

Figure 4: Potential technical roles in a medium organization

Oversee and govern

Work roles identified in the Canadian Cyber Security Skills Framework	Likely assumption of cyber security responsibilities within an SMO
Executive Cyber Leadership	Chief Information Officer (CIO) or Chief Information Security Officer (CISO) and supporting staff
Authorizer	
Cyber Policy and Strategy Planner	
Information Systems Security Manager	Information Systems Manager
Program Manager	Program/Business Line Manager
IT Project Manager	CIO and supporting staff
Product Support Manager	
IT Investment/Portfolio Manager	
Procurement Specialist	
Supply Chain Integrity Analyst	
Financial / Risk Analyst	Chief Financial Officer
Communications Specialist	Communications Officer
Legal Advisor	Legal Counsel
Privacy Officer/Privacy Compliance Manager	
Cyber Instructional Curriculum Developer	Chief Learning Officer or Human Resources Officer

Protect and defend (+DF)

Work roles identified in the Canadian Cyber Security Skills Framework	Likely assumption of cyber security responsibilities within a SMO
Information Systems Security Manager (Cyber Defence Operations)	IT or Systems Manager/Chief Information Officer or Chief Information Security Officer
Cyber defence analyst/Cyber defence infrastructure support	Cyber defence tasks are often included in:
Cyber defence incident responder	• IT help desk/client services
Vulnerability assessor	• System or network administrators
Digital forensics analyst	

2. **Small organization with limited IT dependence and no IT staff**

Most technical work roles would be outsourced, but the primary "oversee & govern" cyber security functions would remain within the organization. This individual would effectively be fulfilling the role of the "security generalist."

Figure 5: Potential outsourced technical roles in a small organization
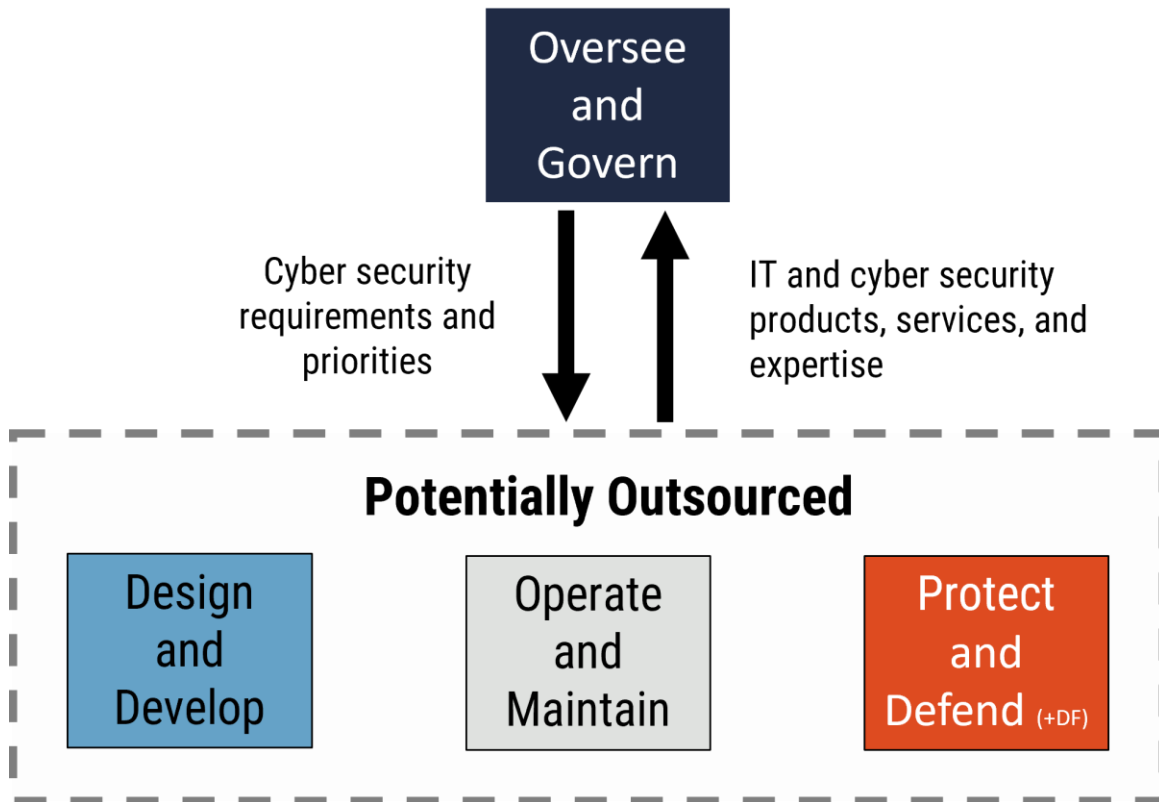
3.3   Cyber security generalist

Within many SMOs and even within larger organizations that are not heavily reliant on Internet-based activities, there are individuals tasked with cyber security responsibilities who may not have any IT or cyber security background.

Given the number of SMOs within the Canadian business landscape, this represents a very large cadre of individuals within the Canadian labour market that have primary responsibility for establishing and managing cyber security within their organizations but may not have any of the discrete roles as defined in the NICE or the Canadian framework. Typically, they:

- perform cyber security functions on a part-time basis in conjunction with other responsibilities

- only require cyber security KSAs to correspond to their business, technical, and threat context

- are not considered cyber security professionals and do not have a cyber security career trajectory

In absence of a term, this framework uses "security generalist" to differentiate them from cyber security specialists identified within the core roles. The security generalist within an organizational setting is typically not a specialist in any
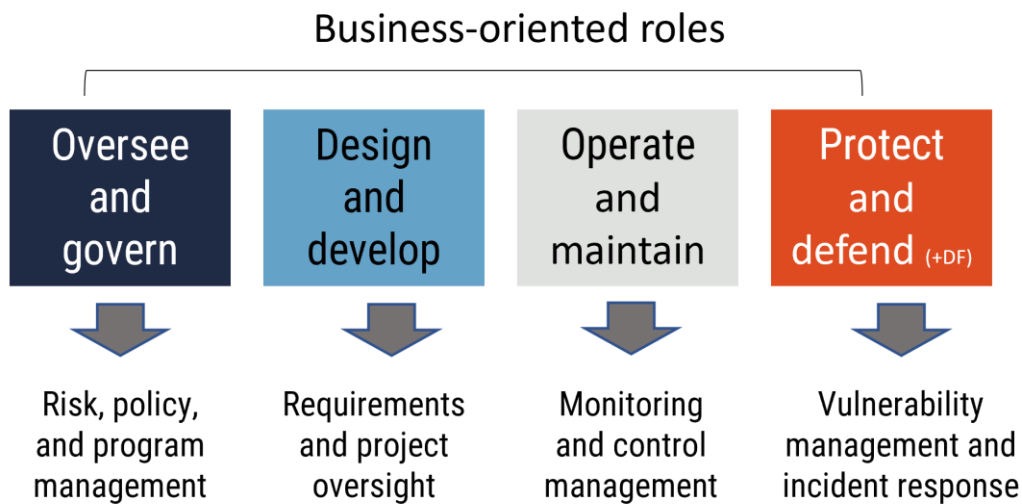
security area, but is often responsible for personnel, physical, contract, and loss prevention security activities as well as cyber security. It's not uncommon, for example, for the chief executive officer (CEO), chief information officer (CIO), chief financial officer (CFO), corporate security officer, human resources manager, or senior administrative official to assume such a role.

Common tasks include:

- Assessing the organization's cyber security posture

- Facilitating identification of organizational cyber risks

- Identifying non-technical cyber security controls

- Identifying and liaising with technical experts, internal or external, on technical controls

- Developing organizational cyber security plans and policies

- Advising leadership on security awareness and training

- Monitoring and support technical experts, whether in-house or outsourced, in their cyber security functions

- Coordinating cyber security incident response

- Monitoring and reporting on response and mitigation actions and recommend courses of action based on technical advice

- Coordinating post-mortem activities on events and incidents, integrating lessons learned into organizational policies and procedures

For many of these tasks, there are ample online resources available to guide the security generalists in their duties. Underpinning effectiveness in these tasks, however, are KSAs needed to support decision making and action. It's unlikely that they will have any extensive cyber security training or education. Accordingly, they should be offered sufficient learning opportunities to attain the required competencies required for their roles as well as the potential threats, necessary technical skills, and business requirements. As shown in the examples in Figure 6, this typically requires competencies borrowed from some of the work roles within each major work category.

Figure 6: Security generalist functions

Business-oriented roles

Oversee and govern	Design and develop	Operate and maintain	Protect and defend (+DF)
Risk, policy, and program management	Requirements and project oversight	Monitoring and control management	Vulnerability management and incident response

Basic knowledge

- Technical context (e.g. organizational IT infrastructure, software, devices, and policies)

- Cyber threat context (including deliberate, accidental, natural hazards)

- Business context (priorities, objectives, market, trends)

- Legal, policy, and ethical context for security

- Cyber security risk management as part of organizational risk

- Cyber security incident management (domain-specific)

- Cyber security processes, technology, trends, and emerging issues

- Sources of cyber security expertise and resources

Basic skills and abilities

- Providing business advice within the legal and policy cyber security context

- Exercising foresight and security planning to support digital business activities and growth

- Translating cyber risk to corporate risk

- Differentiating between compliance and risk

- Interpreting threat and risk assessments for the business context

- Assessing effectiveness of security controls against organizational security objectives

Common competencies

For all core cyber security roles regardless of activity area/work category, there are a number of common competencies that are applied at the basic, intermediate, or advanced level depending on the role. All cyber security professionals, regardless of role, should have a basic ability to apply the following in their work domain/context:

- IT systems and networking

- Systems architecture and models

- Internet protocols, systems and devices

- Cyber security foundations

  - Integrated security framework

  - Cyber security strategies and approaches

  - Threat landscape and common threat surfaces (personnel, physical, IT/logical, supply chain)

  - Cyber threat intelligence process and sources

  - Cyber security analytics

  - Cyber security management policies, processes, and best practices

  - Cyber security systems, tools, and applications

  - Legislation and compliance (e.g. privacy, information sharing, reporting, mandatory standards, etc.)

  - National and industry standards

- Problem-solving and complex thinking in dynamic environments

- Maintaining broader security situational awareness

- Self-awareness regarding knowledge, skills, and abilities required to respond to business, threat, and technical changes

3.4   Core cyber security roles

Recognizing that cyber security is a shared responsibility, this publication describes the cyber security occupation in terms of work that is typically conducted full-time and requires unique KSAs relative to other occupations. Moreover, as per the Canadian Cyber Security Skills Framework, the cyber security occupation is further defined in terms of titles/work roles that are relevant to the Canadian labour market and broader business community. These fall within four major cyber security activity areas or work categories: oversee & govern, design & develop, operate & maintain, and protect & defend. These activity areas/work categories and the inherent work roles are further defined in Annexes A, B, C and D (available upon request).

The core cyber security roles are divided into major work categories/occupational sub-groups similar to those established in the NICE framework[4].

---

[4] Of note, the work categories of Investigate, Analyze and Collect and Operate are only summarized within this document as they are fully defined within the NICE framework and typically fall within the responsibility of military and policing occupations.

- **Oversee & govern:** Overarching responsibility for this occupational sub-group is leadership and management of the cyber security program. This includes technical and non-technical roles.

- **Design & develop (securely provision in the NICE):** This occupational sub-group supports design and development of the digital infrastructure, systems and software. This includes largely technical roles.

- **Operate & maintain:** The primary responsibility of this occupational sub-group is ensuring secure operations of the digital systems and data management. All roles within this sub-group are technical roles.

- **Protect & defend:** This occupational sub-group is focused on cyber security operations. All roles within this occupational sub-group are technical roles.

Common competencies (cyber security professional foundations)

For all the core cyber security roles regardless of activity area/work category, there are a number of common competencies that are applied at the basic, intermediate, or advanced level depending on the role (as listed in Section 3.2). All cyber security professionals, regardless of role, should have a basic ability to apply the following additional competencies in their work domain/context:

- Continuous learning to support currency in knowledge of emerging threats, technological innovations in security, and the changing cyber security landscape

- Communications (oral and verbal) suited to organizational context including drafting and writing technical reports

- Strategic thinking and business acumen to include understanding the business and risk context for cyber security

- Teamwork/collaborating with others including non-cyber security professionals

- Ethics and professional responsibilities

- Cyber security training and awareness within their domain

3.5   Cyber security adjacent roles

There are also numerous roles associated with other organizational functions that typically contribute to organizational cyber security outcomes on a part-time or ad hoc basis[5]. These are cyber security adjacent roles where some cyber security KSAs are required, but they are not typically considered cyber security specialists[6]. For example, in most organizations, a business or policy analyst will likely be employed on a broad range of issues, only some of which will be in support of organizational cyber security. This is not to detract from their role in supporting organizational cyber security, but only to suggest that their work involves often much more than strictly cyber security.

Similarly, executives, program managers, policy analysts, financial analysts, communications specialists, enterprise architects, IT technicians, etc., may have cyber security responsibilities but do not have full time cyber security functions and

---

[5] This is exclusive of 'users' who have ongoing cyber security responsibilities regardless of organizational role
[6] There are some professions/roles where they may be employed full-time within cyber security and are considered specialists, such as those employed in cyber-related law, privacy or ethics. As they are already part of another occupation and are not often part of an organization's workforce, they are not represented in this framework. They are, however, represented in the NICE framework.

are not considered core cyber security roles in this publication. These roles are identified in Annex E (available upon request). A sampling of typical cyber security adjacent work roles is provided in Table 1 below. While they have cyber security responsibilities and require specific cyber security knowledge, skills, and abilities, their primary responsibilities are often either broader or focused on other activities that are not directed towards cyber security. Note that the "protect & defend" category is not included in the figure as that activity area or work category is exclusively employed in cyber security.

Table 1:   Sampling of typical cyber security adjacent work roles

Oversee and govern	Design and develop	Operate and maintain
Chief information or technical officer	Enterprise architect	Systems manager
Corporate security officer	System requirements planner	Systems administrator
Program manager	Business analyst	Systems analyst
IT project manager	Software developer//programmer	Database administrator
Financial analyst	Control systems analyst	Data systems analyst
Learning and development specialist (e.g. security awareness & training)	Web developer	Technical support specialist

4 Summary of the Canadian Cyber Security Skills Framework and attributes

The Canadian Cyber Security Skills Framework (Figure 1) supports an organizational security lens on the NICE framework. The Canadian framework accordingly emphasizes four of the original seven work categories which represent the majority of cyber security work within the Canadian businesses and industries. Each of the work categories represent a responsibility area within cyber security and they are all interconnected.

Leveraging the core elements and characteristics of the NICE framework, the Canadian Cyber Security Skills Framework succeeds in that it:

- helps to better specify the cyber security workforce gaps that exist in the Canadian labour market by applying a business lens onto the NICE framework and distinguishing between core cyber security roles and organizational roles which have some cyber security responsibilities, or cyber security adjacent roles

- simplifies the representation of cyber security related work that is common within most organizations

- is readily adapted to support broader or generalist responsibilities common within SMOs as they aim to address foundational IT and cyber security requirements

- parses out the work categories of "analyze", "collect & operate", and "investigate" that focus on national security and law enforcement roles

- uses commonly understood terms familiar to the broader business and IT community, in particular using design & develop in place of "securely provision"

- maintains emphasis on cyber security responsibilities of adjacent work roles within "oversee & govern", "design & develop" and "operate & maintain"

- recognizes the central role within cyber security operations in "protect & defend"

5 Conclusion

The NICE framework is a comprehensive representation of the cyber security workforce though it's primarily representative of U.S. federal government workforce structure. While it's evolving and private sector stakeholders are becoming more engaged, some of the concerns with directly applying the NICE framework to the Canadian labour market have been discussed within this publication.

The Canadian Cyber Security Skills Framework is a simpler presentation of cyber security work represented within the majority of private and smaller public sector organizations and focuses more closely on business and industry gaps. This framework leverages an organizational security lens, rather than a national security lens, to help better translate cyber security work for businesses and industry. It also serves as a business-oriented interface to the comprehensive and detailed information in the NICE framework.

Overall, this should help to better guide workforce development stakeholders in addressing the cyber security skills deficit.

6 Supporting content

6.1 List of abbreviations

Term	Definition
AI	Artificial Intelligence
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CTA	Cyber Talent Alliance
KSA	Knowledge, skills, and abilities
ICS	Industrial Control Systems
IT	Information Technology
NICE Framework	NICE Framework: NICE Workforce for Cybersecurity
NIST	National Institute of Standards and Technology
NOC	National Occupation Classification
NOS	National Occupation Standards
SCADA	Supervisor Control and Data Acquisition
SMO	Small and medium organizations

6.2 Glossary

For a detailed description of NICE categories, specialty areas and work roles, please refer to NICE framework.

Term	Definition
Ability	Ability is competence to perform an observable behaviour or a behaviour that results in an observable product.
Categories	In terms of the NICE framework, the Categories provide the overarching organizational structure of the NICE framework. There are seven Categories, and all are composed of Specialty Areas and work roles
Competency	The capability of applying or using knowledge, skills, abilities, behaviours, and personal characteristics to successfully perform critical work tasks, specific functions, or operate in a given role or position.
Cyber security	Cyber security is the protection of digital information and the infrastructure on which it resides.
Cyber threat	A cyber threat is an activity intended to compromise the security of an information system by altering the availability, integrity, or confidentiality of a system or the information it contains.
Cyber threat actor	Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks. The

Term	Definition
	globalized nature of the Internet allows these threat actors to be physically located anywhere in the world and still affect the security of information systems in Canada.
Knowledge	Knowledge is a body of information applied directly to the performance of a function.
National Institute for Standards and Technology (NIST)	A part of the U.S. Department of Commerce, U.S. NIST is the federal standards body with the mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
Offensive cyber operations (a.k.a. active cyber operations)	Within the U.S., these are cyber operations intended to project power by the application of force in and through cyberspace. Within Canada, active cyber operations are legislated though Bill C-59 and mandated by the Communications Security Establishment which under ministerial authority will carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.
Security operations centre (SOC)	A SOC provides operational and other security services to the department including the protection of people, property, assets and information. The SOC usually contains the facilities within which system operators can monitor, display and manage information (applications, video, and alarm systems) and then dispatch and respond to events. The design and development of a SOC should identify all areas to accommodate personnel, equipment and supplies associated with control, alarm and event monitoring activities.
Skill	Skill is often defined as an observable competence to perform a learned psychomotor act. Skills in the psychomotor domain describe the ability to physically manipulate a tool or instrument like a hand or a hammer. Skills needed for cyber security rely less on physical manipulation of tools and instruments and more on applying tools, frameworks, processes, and controls that have an impact on the cyber security posture of an organization or individual.
Small and medium organization (SMO)	Organizations that have less than 499 employees.
Speciality area	Within the NICE framework, there are 32 specialty areas. Each specialty area represents an area of concentrated work, or function, within cyber security and related work.
Work role	Within the NICE framework, work roles are the most detailed groupings of cyber security and related work which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.

6.3   References

Number	Reference
1	Canadian Centre for Cyber Security, National Cyber Threat Assessment 2020, November 2020.
2	National Institute of Standards and Technology, NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework, August 2017.
3	National Institute of Standards and Technology, NIST Special Publication 800-181 Revision 2, Workforce Framework for Cybersecurity (NICE framework), November 2020.