Reports of the Auditor General of Canada
to the Parliament of Canada

Report 7

Cybersecurity of Personal Information in the Cloud

Independent Auditor's Report | 2022

Office of the Auditor General of Canada

Bureau du vérificateur général du Canada

Performance audit reports

This report presents the results of a performance audit conducted by the Office of the Auditor General of Canada (OAG) under the authority of the *Auditor General Act*.

A performance audit is an independent, objective, and systematic assessment of how well government is managing its activities, responsibilities, and resources. Audit topics are selected on the basis of their significance. While the OAG may comment on policy implementation in a performance audit, it does not comment on the merits of a policy.

Performance audits are planned, performed, and reported in accordance with professional auditing standards and OAG policies. They are conducted by qualified auditors who

- establish audit objectives and criteria for the assessment of performance
- gather the evidence necessary to assess performance against the criteria
- report both positive and negative findings
- conclude against the established audit objectives
- make recommendations for improvement when there are significant differences between criteria and assessed performance

Performance audits contribute to a public service that is ethical and effective and a government that is accountable to Parliament and Canadians.

This publication is available on our website at www.oag-bvg.gc.ca.

Cette publication est également offerte en français.

Cat. No. FA1-27/2022-1-7E-PDF

ISBN 978-0-660-45993-6

ISSN 2561-343X

Cover photo: alice-photo/Shutterstock.com

Table of Contents

Introduction

Background

Moving government information and services to the cloud

7.1 "The cloud" refers to computer servers that people access over the Internet and the software applications and databases that run on them. Despite their name, cloud servers are physically located in data centres all over the world. The organizations that use them, including the Government of Canada, do not need to own, run, or maintain their own physical servers or software applications. They can use cloud servers and applications on demand, paying for only what they need.

7.2 The Treasury Board of Canada Secretariat released the Government of Canada Cloud Adoption Strategy in 2016 and updated it in 2018. The strategy directs departments (federal organizations) to consider the cloud as the preferred option for delivering information technology services. According to the secretariat, the benefits of cloud computing include

- economies of scale
- on-demand services
- flexibility
- services governed by contracts
- security

7.3 The strategy notes that cloud service providers and the federal departments that use their services share the responsibility for security. Federal departments remain accountable for the confidentiality, integrity, and availability of information technnology services and of related information that a cloud-service provider hosts. The Treasury Board of Canada Secretariat's Digital Operations Strategic Plan: 2018–2022 recognizes that to minimize security risks, departments that use cloud services must build cloud-savvy workforces.

7.4 From April 2018 to March 2022, Shared Services Canada awarded contracts to and Public Services and Procurement Canada established **supply arrangements**[1] with a total of 14 cloud service providers. During that time, several departments began to move their software applications and databases to the cloud. Some also

1 **Supply arrangement**—A method used by Public Services and Procurement Canada to procure goods and services by prequalifying suppliers and establishing the basic terms and conditions that will apply to any resulting contract.

launched cloud-based applications. From April 2018 to March 2021, federal organizations reported spending a total of $210 million on cloud services.

Securing information in the cloud

7.5 Cyberattacks can result in service shutdowns and the failure or destruction of critical infrastructure, such as banking and electrical power distribution. They can also expose personal data, damage reputations, lead to financial costs, significantly disrupt Canadian businesses, and cause financial hardship to individuals. Geopolitical events (such as the invasion of Ukraine) and international commercial conflicts can increase cybersecurity risks significantly. The media have reported many examples of security breaches of cloud systems.

7.6 Because federal organizations have started moving software applications and databases to the cloud, some Canadians' personal information is stored there. To protect information in the cloud, the government has implemented a shared responsibility model that relies on a number of parties to work together.

Roles and responsibilities

7.7 **Treasury Board of Canada Secretariat.** The secretariat provides policy and guidance on cloud services, such as that contained in the Government of Canada Cloud Adoption Strategy. It also coordinates government-wide cybersecurity responses to incidents as outlined in the Government of Canada Cyber Security Event Management Plan.

7.8 **Shared Services Canada.** As a provider of common services to government, this department provides other federal departments with access to approved cloud service providers through contracts that it administers. It also manages and monitors most of the Government of Canada's computer servers and data centres and ensures secure cloud access.

7.9 **Public Services and Procurement Canada.** As a provider of common services to government, this department establishes supply arrangements with prequalified cloud service providers to allow other departments to obtain the software services they offer. In some cases, departments can procure these services directly with these or other providers. For contracts that exceed certain financial thresholds, Public Services and Procurement Canada establishes and administers the contract on a department's behalf. It also assesses the physical security controls of cloud service providers and their personnel.

7.10 **Communications Security Establishment Canada.** As part of this agency, the Canadian Centre for Cyber Security provides Canadians with advice, guidance, services, and support on cybersecurity. This includes conducting security assessments of cloud service providers that Shared Services Canada and Public Services and Procurement Canada have identified for some of their cloud-based procurement processes. It also monitors cloud security and departmental networks and provides training, advice, and guidance on cloud security. It helps federal organizations implement secure digital infrastructures.

7.11 **Individual departments.** Departments (federal organizations) implement their own **security controls**[2] and monitor information and user activity on their own software applications. They are ultimately responsible and accountable for security risks that arise through their use of cloud services. Departments are required to share information about privacy breaches with the Treasury Board of Canada Secretariat and the Office of the Privacy Commissioner of Canada.

Focus of the audit

7.12 This audit focused on whether the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, Communications Security Establishment Canada, and selected federal departments had adequate, effective governance, guidance, and tools in place to prevent, detect, and respond to cybersecurity events that could compromise Canadians' personal information in the cloud. For national security reasons, this report does not name the selected federal departments.

7.13 We examined software applications and databases stored in the cloud that a number of departments use. We also looked at whether the federal government met its commitments to the environment and sustainable development in its procurement of cloud services. We did not examine the security of information that is stored on-premises in government data centres.

7.14 This audit is important because federal departments are increasingly moving software applications and databases into the cloud, including some that handle or store Canadians' personal information. Departments must work together to protect this information from a number of risks, including cyberattacks.

7.15 More details about the audit objective, scope, approach, and criteria are in **About the Audit** at the end of this report.

2 **Security control**—Any type of safeguard or protective countermeasure used to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. We refer to these as "controls" in this report.

Findings and Recommendations

Overall message

7.16 Information stored digitally, whether on-premises in data centres or in the cloud, is exposed to risks of being compromised. Overall, we found that the requirements the government had in place to reduce the security risks of storing information in the cloud were not always followed by the departments we audited. In addition, these requirements and their corresponding roles and responsibilities were not always clear, resulting in inconsistent implementation and increased risks. This is important because the Treasury Board of Canada Secretariat has directed departments to consider moving applications and databases to the cloud, so increasing amounts of Canadians' personal information are moving there. At the same time, cyberattacks are becoming more frequent and sophisticated. The risk of significant impacts on the government and its operations is growing.

7.17 The government must take immediate action to strengthen how it prevents, detects, and responds to cyberattacks. It should do this now, while departments are still in the early stages of moving personal information to the cloud. This action includes strengthening key security controls to prevent, detect, and respond to security breaches. It also includes clarifying shared roles and responsibilities for cybersecurity—which are highly complex in a cloud environment—so that all departments know exactly what they should be doing.

7.18 We also found that, 4 years after the Treasury Board of Canada Secretariat first directed departments to consider moving to the cloud, it had still not provided a long-term funding approach for cloud adoption. It had also not given departments tools to calculate the costs of moving to or of operating in the cloud and securing the information stored in it. Departments need both a funding approach and costing tools to ensure that the people, expertise, skills, training, funding, and other resources they need to secure cloud-based information are available to prevent and address the greatest threats and risks. A funding approach and costing tools are essential for cloud adoption and would strengthen Canada's cyber-defence capabilities both at the departmental level and government-wide.

Securing personal information in the cloud

There were weaknesses in departments' controls for preventing, detecting, and responding to cyberattacks

What we found

7.19 We found gaps in Shared Services Canada's and Public Services and Procurement Canada's use of controls to prevent cybersecurity breaches. These findings relate to security inspections and some aspects of cloud guardrails, a type of security control. We cannot report these findings publicly because doing so could reveal vulnerabilities and pose a risk to national security. Instead, we have reported them directly to the departments.

7.20 We also found shortcomings in controls for detecting and responding to cybersecurity breaches. For example, we found that the Treasury Board of Canada Secretariat conducted few simulations to test or improve the Government of Canada Cyber Security Event Management Plan, which outlines how to respond to cybersecurity breaches that affect multiple departments. In addition, we found that individual departments did not have their own departmental cybersecurity event management plans in place, nor did they fully define their roles and responsibilities for managing incidents.

7.21 Finally, we found that contract security clauses were unclear and not standardized. During our audit, Shared Services Canada and Public Services and Procurement Canada began working to address these issues.

7.22 The following topics present the analysis supporting these findings:

- Gaps in security inspections
- Cloud guardrails not validated or monitored consistently across all contracts
- Contract security clauses unclear and not standardized
- Shortcomings in cybersecurity event management plans and their use

Why this finding matters

7.23 This finding matters because cybersecurity breaches are on the rise, and strong controls to prevent, detect, and respond to them can reduce the risk of breaches and limit compromises of Canadians' personal information when they do occur.

Context

7.24 Each department is responsible for managing its own cybersecurity risks and implementing security controls. But departments also rely on several central departments to implement certain security controls for preventing, detecting, and responding to breaches. As a result, there is a high level of shared responsibility across the federal government for managing the cybersecurity of personal information in the cloud. We looked at these responsibilities for 4 categories of security controls (Exhibit 7.1). A cloud guardrail (exhibits 7.1 and 7.2) is a type of security control.

Exhibit 7.1—A variety of federal government departments share responsibilities for key cloud security controls

Control	Purpose	Roles and responsibilities
Security assessments of cloud service providers	To determine whether providers' personnel, physical equipment, and services meet Government of Canada security requirements	• Public Services and Procurement Canada is responsible for inspecting the physical facilities where cloud service providers keep the servers that store protected information. • Departments must verify and monitor a cloud service provider's compliance, according to the results of Public Services and Procurement Canada's inspection, before they authorize these facilities to process, store, or transmit data that could include Canadians' personal information. These assessments and reassessments must be timely and complete because as technology changes, departments face new issues and risks to understand, consider, and mitigate.
Cloud guardrails	To protect data that is stored or transmitted through networks in the cloud	• Departments must implement these guardrails according to the Treasury Board Directive on Service and Digital. • Shared Services Canada **validates**[3] the implementation of the guardrails, monitors departmental compliance with the guardrails on a monthly basis, and reports any non-compliance to the Treasury Board of Canada Secretariat. If guardrails are not implemented and applied consistently across departments, there is an increased risk that attackers could exploit vulnerabilities. Periodic monitoring also helps maintain consistent security. Security weaknesses may go unnoticed or unchecked if monitoring is only partially done.

3 **Validate**—In the context of validating guardrails, the process of reviewing evidence to confirm that departments have implemented the guardrails as required by the Treasury Board Directive on Service and Digital.

Control	Purpose	Roles and responsibilities
Security clauses in cloud contracts and supply arrangements	To identify security requirements and responsibilities before a department begins using cloud services	• Shared Services Canada establishes contracts, and Public Services and Procurement Canada establishes supply arrangements with cloud service providers. These define the security requirements for managing accounts, incidents, and vulnerabilities and for monitoring systems. The absence of standard clauses in cloud security contracts and supply arrangements can lead to inconsistent contracting practices and result in insufficient security safeguards.
Cybersecurity event management plans and exercises	To outline how to detect and respond to security breaches at the departmental level and government-wide	• The Treasury Board of Canada Secretariat provides the Government of Canada Cyber Security Event Management Plan to detect, respond to, and limit the consequences of an attack on an organization's information and technology systems. • Departments must also have plans with similar procedures. These plans are critical for protecting information and technology assets against cyber threats because they provide policies, procedures, roles and responsibilities, and guidance that minimize response times and reduce the chance of confusion.

Analysis to support this finding

Gaps in security inspections

7.25 We found gaps in the way security inspections for cloud service providers were carried out. We cannot report our findings publicly because doing so could reveal information on vulnerabilities and pose a risk to national security. Consequently, we reported them directly to Public Services and Procurement Canada. Our findings include a recommendation to Public Services and Procurement Canada relating to the communication of physical security inspection results to stakeholders and the renewal of physical security inspections.

Cloud guardrails not validated or monitored consistently across all contracts

7.26 Cloud guardrails are a minimum set of controls that departments must implement to prevent and detect cyberattacks in their cloud environments. The 12 cloud guardrails shown in Exhibit 7.2 are meant to enhance security in cloud-based environments.

Exhibit 7.2—The Government of Canada established 12 cloud guardrails that serve as a minimum set of security controls

Cloud guardrails	Objective
1. Protect root/global administrator account	Protect the root or master account that was used to establish the cloud service.
2. Management of administrative privileges	Establish access control policies and procedures to manage administrative privileges.
3. Cloud console access	Limit access to authorized users and Government of Canada devices.
4. Enterprise monitoring accounts	Create role-based accounts to enable enterprise monitoring and visibility.
5. Data location	Establish policies to restrict sensitive Government of Canada applications and information to approved geographic locations.
6. Protection of data at rest	Protect data at rest by default (for example, storage) for cloud-based applications.
7. Protection of data in transit	Protect data transit networks by using appropriate encryption and network safeguards.
8. Segment and separate	Segment and separate information according to its sensitivity.
9. Network security services	Establish external and internal network perimeters, and monitor network traffic.
10. Cyber-defence services	Establish a memorandum of understanding for defensive services and threat-monitoring protection services.
11. Logging and monitoring	Enable logging of network and system information and events for the cloud environment and for cloud-based workloads.
12. Configuration of cloud marketplaces	Restrict the use of commercial software from third-party cloud service providers to products approved by the Government of Canada.

Source: Adapted from Government of Canada Cloud Guardrails, Government of Canada

7.27 The Treasury Board Directive on Service and Digital requires departments that contract with cloud service providers to implement cloud guardrails before using cloud services and to ensure they remain in place. The directive does not include contracts with cloud service providers outside of those established by Shared Services Canada, such as those set up with providers who were prequalified under a Public Services and Procurement Canada supply arrangement. The Treasury Board of Canada Secretariat is responsible for overseeing and enforcing departments' compliance with the guardrails. The secretariat can revoke a department's cloud access if it does not implement the guardrails.

7.28 We found that for contracts that Shared Services Canada set up between departments and cloud service providers, it checked whether departments implemented the guardrails within the first 30 days. However, it performed only limited ongoing monitoring after that. We also found that for cloud services that were set up by Public Services and Procurement Canada, no one validated whether departments put guardrails in place initially, and no one monitored ongoing compliance. In our view, this inconsistent application of controls across government increases the risk that Canadians' personal information in the cloud could be compromised.

7.29 We reviewed Shared Services Canada's validation of how departments implemented guardrails. We found that the department did not assess some controls effectively and sometimes gave departments passing grades even when they did not implement the guardrails properly. The following are 2 examples:

- Guardrail 6 (on the protection of data at rest) requires departments to seek guidance from privacy officials before storing personal information in cloud-based environments. However, we found that Shared Services Canada did not verify whether departments did so.
- Guardrail 8 (on segmenting and separating information) requires departments to provide technical diagrams of their network security designs to assessors who are expected to evaluate them for completeness and accuracy. However, we found a case where an assessor verified only that a diagram had been provided, not whether it was complete or accurate.

7.30 We found that although Shared Services Canada validated all departments' implementation of the 12 guardrails within the first 30 days of their contracts with cloud service providers, it monitored only 2 of the 12 guardrails for ongoing compliance. Furthermore, for these 2, it verified only administrative aspects (such as those related to billing and reporting), not whether the guardrails were still in place and working as intended. Shared Services Canada left the ongoing monitoring of guardrails from a security perspective up to individual departments.

7.31 **Recommendation.** In consultation with Shared Services Canada and Public Services and Procurement Canada, the Treasury Board of Canada Secretariat should do the following:

- Extend the requirement for guardrails to cloud service provider contracts that stem from supply arrangements established by Public Services and Procurement Canada.
- Clarify who is responsible for the initial validation and ongoing monitoring of cloud guardrail controls and what processes they should follow.

The Treasury Board of Canada Secretariat's response. *Agreed.*

See **Recommendations and Responses** at the end of this report for detailed responses.

Contract security clauses unclear and not standardized

7.32 We found that the contracts for cloud services put in place by Shared Services Canada and the supply arrangements established by Public Services and Procurement Canada included only limited details about providers' obligations during security incidents, such as who should respond and how quickly.

7.33 From April 2018 to March 2022, the departments set up cloud contracts or supply arrangements with 14 cloud service providers. We reviewed all of these and found that, although the arrangements set out some security and privacy obligations, neither department provided sufficient detail about the departments' or cloud service providers' obligations for handling security incidents and privacy breaches, including how quickly either party should respond and who should communicate incidents and breaches (and to whom).

7.34 We also found that neither department included standard security clauses or conditions in the contracts and supply arrangements they established. However, both have since recognized the need to develop these to avoid conflicting contracting approaches and duplicated efforts. In February 2022, the departments, along with the Treasury Board of Canada Secretariat and Communications Security Establishment Canada, formed a Cloud Procurement Working Group to accomplish the following tasks:

- Develop a Government of Canada cloud procurement approach, including standardized terms and conditions templates.
- Standardize roles and responsibilities in the cloud procurement process.
- Clarify cloud contract security requirements within the federal government.

Shortcomings in cybersecurity event management plans and their use

7.35 When a cybersecurity event occurs, the lead security agencies and individual departments need to be able to respond quickly and in a coordinated manner. To do this, they need to have cybersecurity event management plans in place that have been tested and proven effective through simulation exercises. The government's ability to detect and respond to cyberattacks government-wide relies on the ability of each department to do so at its level.

7.36 The Government of Canada Cyber Security Event Management Plan took effect in April 2020, replacing a previous version published in January 2018. It explains the roles and responsibilities of the departments and central agencies tasked with coordinating responses

to government-wide events. It covers steps to assess, classify, and escalate events. According to the plan, departments are responsible for continually improving their capacity to respond to cybersecurity events. This includes testing plans and procedures, implementing lessons learned, maintaining contact lists for individuals who have responsibilities set out in the plan, and training personnel, including cybersecurity personnel.

7.37 In our review of the government's response to a past event, we found that the Treasury Board of Canada Secretariat and Communications Security Establishment Canada performed lessons-learned exercises and developed a report, recommendations, and an action plan to improve future responses.

7.38 However, we found that the Treasury Board of Canada Secretariat did not follow the requirements set out in the Government of Canada Cyber Security Event Management Plan for testing plans and procedures and keeping the plan up to date:

- The secretariat did not update or renew the plan, despite its own requirements to test, modify, and review it annually. It drafted a new version in October 2021 but had not tested or adopted it at the time of our audit.
- The secretariat organized tabletop simulations to test and improve the effectiveness of the plan. However, it has conducted only 3 of these exercises since 2018 (approximately 1 every 17 months), well short of the minimum recommended frequency of once every 12 months. Regular simulations are needed because of changes in personnel as well as evolving technology and working environments.

7.39 When we reviewed the cybersecurity event management plans for the 3 departments selected for our audit, we found the following:

- Each of the 3 departments conducted annual tabletop exercises and tests of the security of its applications.
- Each of the 3 departments drafted plans, but 2 out of 3 told us they lacked the funds and capacity to implement them fully.
- Two of the 3 departments did not finish defining their internal roles and responsibilities for managing incidents.
- Although the secretariat began the process of collecting information from departments in September 2021, at the time of our audit, it did not know if all departments had implemented cybersecurity event management plans.

7.40 **Recommendation.** The Treasury Board of Canada Secretariat should do the following:

- Ensure that the Government of Canada Cyber Security Event Management Plan applies to the evolving cloud environment and shared responsibilities, review and test it at least annually, and update it as needed.
- Follow up annually to ensure that departments finalize, implement, and regularly test their security event management plans.

The Treasury Board of Canada Secretariat's response. *Agreed.*

See **Recommendations and Responses** at the end of this report for detailed responses.

The roles and responsibilities for ensuring cloud cybersecurity were unclear and incomplete

What we found

7.41 We found that the Treasury Board of Canada Secretariat's Government of Canada Cloud Roles and Responsibilities Matrix, which is the main tool used by the secretariat to communicate about shared cloud roles and responsibilities, left out important information that departments need to carry out their cybersecurity obligations properly. As a result, the organizations were unclear about who should do what in certain areas, such as who should evaluate the information technology security controls for data residency requirements.

7.42 The analysis supporting this finding discusses the following topic:

- Departments confused on cybersecurity roles

Why this finding matters

7.43 This finding matters because while individual departments are ultimately responsible and accountable for the security risks resulting from their use of cloud services, the security of personal information in the cloud depends on a shared responsibility model that includes departments and cloud service providers. To prevent security breaches and respond quickly and effectively if one does occur, accountabilities, roles, and responsibilities must be clear. If there are gaps or uncertainty, departments may not understand or properly carry out their cybersecurity responsibilities.

Context

7.44 The Treasury Board of Canada Secretariat communicates its decisions about roles and responsibilities for cloud usage and storage by departments through the Government of Canada Cloud Roles and Responsibilities Matrix that it makes available to departments. The intent of a matrix is to map out how departments are meant to share responsibilities in all areas of cloud adoption, including security.

Analysis to support this finding

Departments confused on cybersecurity roles

7.45 We found that the Treasury Board of Canada Secretariat's Government of Canada Cloud Roles and Responsibilities Matrix did not include or modify cloud roles and responsibilities that have evolved or been added since March 2018, when the matrix was last updated. Here are 4 examples:

- The secretariat did not include the implementation and validation of cloud guardrails in its matrix.
- Communications Security Establishment Canada is responsible for assessing the information technology security controls of cloud service providers. However, we found that after the matrix was implemented, departments also had the option to perform some of these assessments themselves. It is not clear if the agency should be monitoring or supervising the departments' assessments.
- Communications Security Establishment Canada's responsibilities for monitoring cloud activity to detect and respond to cybersecurity events and to inform and support compromised departments do not appear in the matrix.
- The matrix does not include the secretariat's responsibility to coordinate government-wide security event management exercises.

7.46 The roles and responsibilities for cloud security are articulated in multiple documents. As a result, we found that departments were confused about some of their roles and responsibilities. For example, the Directive on Service and Digital says departments are responsible for ensuring that data stored in the cloud, including sensitive and personal information, resides in Canada. Yet, after having reviewed the contracts and supply arrangements established by Shared Services Canada and Public Services and Procurement Canada, we found that not all parties involved understood this:

- The 3 selected departments told us they thought that Public Services and Procurement Canada or Communications Security Establishment Canada was responsible for checking on this.

- Public Services and Procurement Canada officials told us that Communications Security Establishment Canada was responsible.
- Communications Security Establishment Canada officials told us this task is up to the chief information officers or data owners at each department.

Without a clear understanding of who ensures that data stored in the cloud resides in Canada, organizations risk not knowing whether personal information ends up stored in a different country and if so, whether it is subject to different (potentially inferior) privacy protection laws and security protocols.

7.47 **Recommendation.** In consultation with Communications Security Establishment Canada, Shared Services Canada, Public Services and Procurement Canada, and departments, the Treasury Board of Canada Secretariat should document and proactively communicate to any department that is using or contemplating cloud services the roles and responsibilities needed to design, implement, validate, monitor, coordinate, and enforce the security controls needed to protect sensitive and personal information in the cloud. The secretariat should review and update these roles and responsibilities at least every 12 months.

The Treasury Board of Canada Secretariat's response. *Agreed.*

See **Recommendations and Responses** at the end of this report for detailed responses.

Providing a costing model and funding approach

The Treasury Board of Canada Secretariat did not provide departments with a costing model or funding approach for cloud services

What we found

7.48 We found that, 4 years after the Treasury Board of Canada Secretariat first directed departments to begin transitioning to the cloud, it had still not given them tools to understand the costs of moving to, operating in, and securing applications in the cloud versus keeping them in a Shared Services Canada data centre. We also found that, when departments chose to host their applications in the cloud instead of at a government data centre, they became responsible for funding the ongoing operation and security of those services. Federal funding for these did not shift to departments from Shared Services Canada after departments adopted cloud services.

7.49 The analysis supporting this finding discusses the following topic:

- No costing model or long-term funding approach

Why this finding matters

7.50 This finding matters because Canadians expect the government to minimize costs, and while cloud services may provide opportunities to do so, without adequate tools, departments cannot conduct cost-benefit analyses to make informed decisions. They may also lack adequate funding for their ongoing cloud activities, including those related to security.

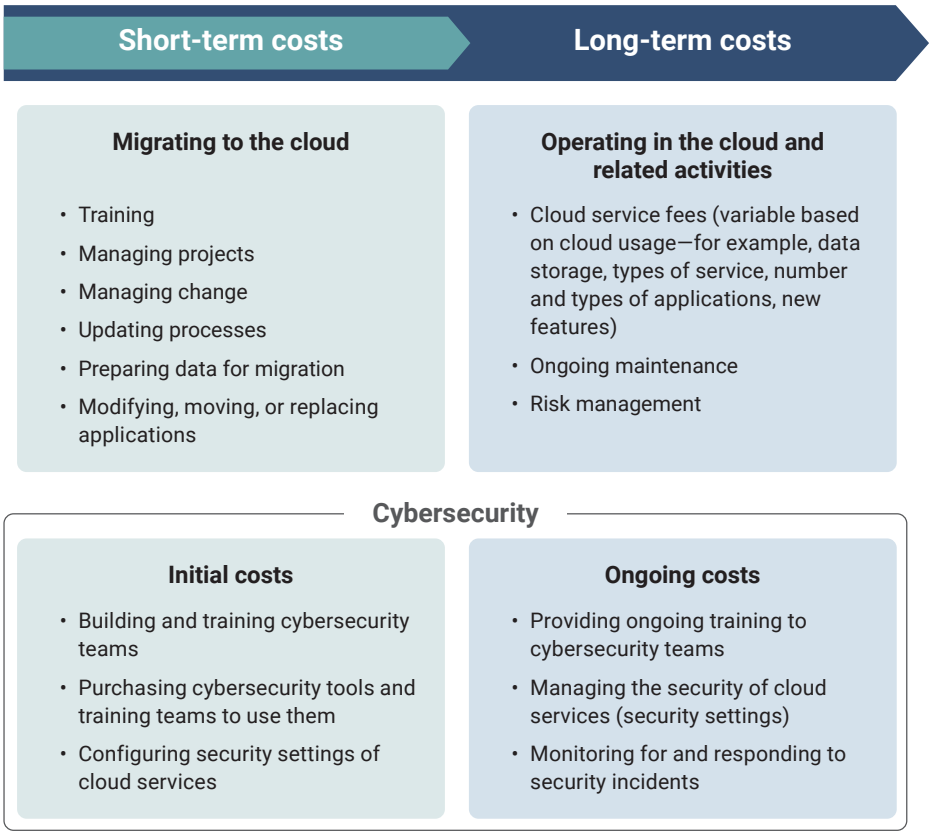
Analysis to support this finding

No costing model or long-term funding approach

7.51 We found that when the Treasury Board of Canada Secretariat released its cloud adoption strategy in 2018, it did not develop or release a long-term funding approach or costing model to go with the strategy, nor did the secretariat have these for us to review during our audit. As a result, we could not determine how these might address departments' known challenges in understanding the costs of moving information to and securing information in the cloud and funding the long-term protection of that information.

7.52 When departments decide whether their applications or services should reside in a data centre hosted by Shared Services Canada or in the cloud, cost is an important consideration. This is because adopting cloud services shifts some of the costs of data storage and application hosting from Shared Services Canada to the departments, which also become responsible for funding the ongoing cloud operations and the cybersecurity responsibilities that come with cloud adoption. These include building teams with cloud and cybersecurity skills, purchasing cybersecurity tools, and maintaining operations and security on an ongoing basis (Exhibit 7.3).

Exhibit 7.3—Cloud adoption comes with short- and long-term cybersecurity costs for departments



Note: These lists are meant to illustrate some of the cost considerations involved. They are not comprehensive.

7.53 Although short-term funding has been made available to departments to migrate their applications to the cloud, working groups and senior government committees have noted that how departments will fund their ongoing cloud operations remains unknown. At the same time, the secretariat told us that departmental spending on cloud services government-wide has increased significantly year over year, to almost $120 million in 2021 from $35 million in 2018.

7.54 To help departments better understand the costs involved in adopting cloud services and to improve their decision making, the secretariat planned to develop a costing model that departments could use to compare the costs of storing data and hosting applications in the cloud versus in Government of Canada data centres. This model would include acquisition costs, ongoing operational activities (such as monitoring and maintaining security), and ongoing cloud service costs. The secretariat also told us that the model would focus on modernizing and hosting existing applications.

7.55 Departments would be able to access funding to modernize technology, adopt new practices, and build the capacity and skills needed for modernization. For any new applications moved to the cloud, departments would have to pay for the associated hosting, operating, and maintenance costs themselves, either by reallocating funds internally or requesting new or additional funding, such as through submissions to the Treasury Board.

7.56 Without long-term funding for ongoing operations, the 3 departments we selected for this audit were using a variety of short-term funding measures to support their cloud and cybersecurity operations, including reallocating funds that had been intended for other purposes. According to the departments, cloud cybersecurity costs increased significantly from the 2020–21 fiscal year to the 2021–22 fiscal year and are expected to remain high in the 2022–23 fiscal year. For example, 1 department told us that its costs more than tripled from the 2020–21 fiscal year to the 2021–22 fiscal year (rising from $200,000 to $700,000) and are likely to remain at that level in the 2022–23 fiscal year. Departments indicated that the need to use short-term funding for cloud and cybersecurity services risks the long-term sustainability of these operations.

7.57 Although larger departments may be able to absorb some of the costs of cloud adoption and security, this approach is likely not sustainable over the long term, and smaller departments may not be able to cover any of these costs. In addition, shifting resources from other information technology operations to fund cybersecurity can put these other information technology operations at risk.

7.58 **Recommendation.** In consultation with Shared Services Canada and other departments, the Treasury Board of Canada Secretariat should do the following:

- Develop and provide a costing model to help departments make informed decisions about moving to the cloud and determine whether additional resources and funding are required.
- Help departments determine their long-term operational funding needs and support their access to funding so they can fulfill their evolving responsibilities for cloud operations, including securing sensitive information in the cloud.

The Treasury Board of Canada Secretariat's response. *Agreed.*

See **Recommendations and Responses** at the end of this report for detailed responses.

Promoting environmental responsibility and sustainable development

Public Services and Procurement Canada and Shared Services Canada did not include environmental criteria in their procurement of cloud services

What we found

7.59 We found that Public Services and Procurement Canada and Shared Services Canada did not include environmental criteria when they procured cloud services, even though both organizations have developed guidance and mandatory training for staff on integrating environmental considerations into the procurement of services, including cloud services.

7.60 The analysis supporting this finding discusses the following topic:

- No environmental criteria for cloud procurement

Why this finding matters

7.61 This is important because the Government of Canada has set a target of net-zero greenhouse gas emissions by 2050, and its policies and actions should be aligned. The lack of environmental criteria in the procurement of cloud services is a missed opportunity for departments to contribute to achieving the target and support the United Nations' 2030 Agenda for Sustainable Development.

7.62 In addition, the Treasury Board of Canada Secretariat and Shared Services Canada have noted that digital technologies are expected to be responsible for 8% of global greenhouse gas emissions by 2025 and for up to 14% by 2040. Not including environmental criteria in the procurement of cloud services creates a risk that cloud adoption will not support the Greening Government Strategy and may even contribute to an increase in emissions.

Context

Ensure sustainable consumption and production patterns

Source: United Nations

7.63 In 2015, Canada committed to achieving the United Nations' 2030 Agenda for Sustainable Development, which sets out 17 Sustainable Development Goals. Goal 12 aims to ensure sustainable consumption and production patterns. One of its targets is to "promote public procurement practices that are sustainable, in accordance with national policies and priorities."

7.64 In 2017, Canada established the Greening Government Strategy with the expectation that all federal government organizations would incorporate environmental considerations into their procurement processes. The strategy recommended that departments encourage suppliers to disclose their greenhouse gas emissions and environmental performance information.

7.65 In 2020, the Greening Government Strategy was presented as a Government of Canada directive. It indicates that Canada intends to achieve net-zero emissions by 2050 in its operations, including the procurement of goods and services. It also indicates that the government would include criteria aimed at reducing greenhouse gas emissions in its procurements for goods and services with a high environmental impact. As noted in the May 2022 Report of the Commissioner of the Environment and Sustainable Development on the Greening Government Strategy, progress to date suggests that the government is falling short on meeting its emission-reduction goal.

7.66 In addition, the 2018 Policy on Green Procurement requires Public Services and Procurement Canada and Shared Services Canada to include environmentally preferable options when procuring services, where feasible. It also requires departments to buy environmentally preferable goods and services where value for money is demonstrated.

7.67 At the time of the audit, the Government of Canada was updating its cloud adoption strategy. The most recent draft, dated February 2022, included 10 items intended to help departments achieve business value. One item involved contributing to the government's overall sustainable development objectives by "providing highly-efficient enterprise-scale infrastructure that reduces [greenhouse] gas emissions and promotes the greening of government."

Analysis to support this finding

No environmental criteria for cloud procurement

7.68 We found that the Treasury Board of Canada Secretariat and Public Services and Procurement Canada developed guidance and training to help contracting officers integrate environmental considerations into the procurement of services. We also found that Public Services and Procurement Canada and Shared Services Canada trained their procurement officers in green procurement.

7.69 However, we found that these departments did not require cloud service providers to demonstrate their environmental performance or to explain how their services would reduce Canada's greenhouse gas emissions. Although the departments requested information from providers about their environmental commitments and the status of their operations, they did not require it or confirm its accuracy when provided.

7.70 We examined 14 contracts and supply arrangements for cloud services and found that none included environmental clauses. In addition, there were no standard environmental clauses relating to cloud services in Public Services and Procurement Canada's Standard Acquisition Clauses and Conditions Manual.

7.71 Public Services and Procurement Canada told us that departments can include their own environmental requirements. However, the selected departments told us they did not write their own contract clauses. They relied on the Standard Acquisition Clauses and Conditions Manual to ensure that clauses were applied consistently across departments.

7.72 **Recommendation.** Public Services and Procurement Canada and Shared Services Canada should include environmental criteria when procuring cloud services to support sustainability in procurement practices and contribute to achieving Canada's net-zero goal.

The departments' response. *Agreed.*

See **Recommendations and Responses** at the end of this report for detailed responses.

Conclusion

7.73 We concluded that the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, Communications Security Establishment Canada, and selected departments had controls at their disposal to prevent, detect, and respond to cybersecurity events that threaten the security of Canadians' personal information in the cloud but did not effectively implement them or establish and communicate clear roles and responsibilities for implementing them.

7.74 We also concluded that the secretariat did not provide a long-term funding approach or costing model to help departments better understand the costs of moving to and operating in the cloud.

7.75 Finally, we concluded that the federal government did not include environmental criteria in its procurement of cloud services, even though it was required to reduce greenhouse gas emissions.

About the Audit

This independent assurance report was prepared by the Office of the Auditor General of Canada on the cybersecurity of Canadians' personal information in the cloud. Our responsibility was to provide objective information, advice, and assurance to assist Parliament in its scrutiny of the government's management of resources and programs, and to conclude on whether the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, Communications Security Establishment Canada (and its Canadian Centre for Cyber Security), and selected departments complied in all significant respects with the applicable criteria.

All work in this audit was performed to a reasonable level of assurance in accordance with the Canadian Standard on Assurance Engagements (CSAE) 3001—Direct Engagements, set out by the Chartered Professional Accountants of Canada (CPA Canada) in the CPA Canada Handbook—Assurance.

The Office of the Auditor General of Canada applies the Canadian Standard on Quality Control 1 and, accordingly, maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

In conducting the audit work, we complied with the independence and other ethical requirements of the relevant rules of professional conduct applicable to the practice of public accounting in Canada, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behaviour.

In accordance with our regular audit process, we obtained the following from entity management:

- confirmation of management's responsibility for the subject under audit
- acknowledgement of the suitability of the criteria used in the audit
- confirmation that all known information that has been requested, or that could affect the findings or audit conclusion, has been provided
- confirmation that the audit report is factually accurate

Audit objective

The objective of this audit was to determine whether the federal government—including the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, Communications Security Establishment Canada (and its Canadian Centre for Cyber Security), and selected departments—had governance, guidance, and tools in place to prevent, detect, and respond to cybersecurity events that could affect Canadians' personal information in the cloud.

We also looked at whether the federal government met its commitments to the environment and sustainable development in its procurement of cloud services. As part of the Office of the Auditor General of Canada's commitment to achieving the United Nations' Sustainable Development Goals, we identified Goal 12 as applicable to the procurement of cloud services because of its target to promote public procurement practices that are sustainable, in accordance with national policies and priorities.

Scope and approach

The audit focused on how government departments share responsibilities for the security of personal information: While individual departments are responsible for managing risk related to organizational cybersecurity and for implementing security controls to mitigate cybersecurity risk in their programs, they rely on lead security agencies for certain security controls. We selected 3 departments that were using cloud services to store or process personal information. We consulted them on the roles and responsibilities of the lead security agencies and examined how all of the departments worked together on cybersecurity.

We identified a variety of key controls that relate to mitigating the risk of security breaches of personal information in cloud-hosted applications and services: security clauses in contracts, guardrail validation, assessments of physical and personnel security controls of cloud service providers, security assessments of cloud service providers' services, the Government of Canada Cyber Security Event Management Plan, and departmental security event management plans. We validated and confirmed these controls with each entity for accuracy, completeness, and relevance. Where applicable, we incorporated these into the audit criteria and conducted additional control testing.

Our audit work included reviewing plans, strategies, policies, and guidelines, interviewing relevant departmental officials, and testing controls to understand the overall practices and systems that the federal government has in place for securing personal information in the cloud. We did the following:

- reviewed the 8 cloud framework agreements established with cloud service providers and tested a sample of 6 cloud supply arrangements to determine whether security requirements (contract clauses) exist with cloud service providers
- examined the validation of cloud guardrails for the selected departments
- reviewed a sample of 14 physical security inspection reports on cloud service providers to determine whether physical inspection procedures were followed and whether results were communicated
- reviewed 1 major security incident to determine whether security event management procedures were followed

We did not examine cloud procurement activities carried out by the selected departments within their own contracting authority limits. We also did not conduct our own information technology security testing or assessments of the selected departments.

Criteria

We used the following criteria to determine whether the federal government—including the Treasury Board of Canada Secretariat, Shared Services Canada, Public Services and Procurement Canada, Communications Security Establishment Canada (and its Canadian Centre for Cyber Security), and selected departments—had governance, guidance, and tools in place to prevent, detect, and respond to cybersecurity events that could affect Canadians' personal information in the cloud.

We also used the following criteria to determine whether the federal government met its commitments to the environment and sustainable development in its procurement of cloud services.

Criteria	Sources
The Treasury Board of Canada Secretariat defines the roles and responsibilities for the cybersecurity of personal information in the cloud.	• Policy on Government Security, Treasury Board • Directive on Security Management, Treasury Board • Policy on Service and Digital, Treasury Board • Directive on Service and Digital, Treasury Board • Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021, Treasury Board of Canada Secretariat • Digital Operations Strategic Plan: 2021–2024, Treasury Board of Canada Secretariat • Government of Canada Cloud Adoption Strategy, Treasury Board of Canada Secretariat, 2018 • Government of Canada Cloud Operationalization Framework, Treasury Board of Canada Secretariat

Criteria	Sources
The Treasury Board of Canada Secretariat has a funding model that ensures departments have the resources they need to protect the cybersecurity of their cloud operations and to detect and respond to threats.	• Policy on Service and Digital, Treasury Board • Directive on Service and Digital, Treasury Board • Policy on the Planning and Management of Investments, Treasury Board, 2019 • Policy on the Planning and Management of Investments, Treasury Board, 2021 • Government of Canada Strategic Plan for Information Management and Information Technology 2017 to 2021, Treasury Board of Canada Secretariat • Digital Operations Strategic Plan: 2018–2022, Treasury Board of Canada Secretariat • Digital Operations Strategic Plan: 2021–2024, Treasury Board of Canada Secretariat • Government of Canada Cloud Adoption Strategy, Treasury Board of Canada Secretariat, 2018 • Budget 2018, Budget 2019, and Budget 2021
Shared Services Canada validates cloud guardrails prior to approving services in the cloud.	• Government of Canada Cloud Guardrails, Government of Canada • Government of Canada Cloud Operationalization Framework, Treasury Board of Canada Secretariat • Direction on the Secure Use of Commercial Cloud Services, Treasury Board of Canada Secretariat • Government of Canada Cloud Security Risk Management Approach and Procedures, Treasury Board of Canada Secretariat • Government of Canada Security Control Profile for Cloud-Based GC Services • Standard Operating Procedure: Validating Cloud Guardrails, Treasury Board of Canada Secretariat, 2019

Criteria	Sources
Public Services and Procurement Canada and Shared Services Canada, together with selected departments, document the contract clauses for security management, roles and responsibilities for security, security monitoring and notification, and data residency requirements.	• Policy on Government Security, Treasury Board • Directive on Security Management, Treasury Board • Policy on Service and Digital, Treasury Board • Directive on Service and Digital, Treasury Board • Guideline on Service and Digital, Treasury Board of Canada Secretariat • Contracting Policy, Treasury Board • Direction on the Secure Use of Commercial Cloud Services, Treasury Board of Canada Secretariat • Direction for Electronic Data Residency, Treasury Board of Canada Secretariat • Government of Canada White Paper: Data Sovereignty and Public Cloud, Treasury Board of Canada Secretariat • Supply Manual, Public Services and Procurement Canada • Contract Security Manual, Public Services and Procurement Canada • Standard Acquisition Clauses and Conditions Manual, Public Services and Procurement Canada • Supply Manual, Shared Services Canada • Technology Supply Chain Guidelines, Canadian Centre for Cyber Security • Guidance on Cloud Security Assessment and Authorization, Canadian Centre for Cyber Security • IT Security Risk Management: A Lifecycle Approach, Canadian Centre for Cyber Security • The 18 CIS Critical Security Controls, Center for Internet Security • COBIT 2019 Framework (Control Objectives for Information and Related Technology), Information Systems Audit and Control Association

Criteria	Sources
Public Services and Procurement Canada screens cloud service providers' physical locations and personnel for security and data residency requirements and repeats this screening periodically.	• Policy on Government Security, Treasury Board • Directive on Security Management, Treasury Board • Direction on the Secure Use of Commercial Cloud Services, Treasury Board of Canada Secretariat • Direction for Electronic Data Residency, Treasury Board of Canada Secretariat • Government of Canada White Paper: Data Sovereignty and Public Cloud, Treasury Board of Canada Secretariat • Policy on the Contract Security Program, Public Services and Procurement Canada, 2019 • Supply Manual, Public Services and Procurement Canada • Contract Security Manual, Public Services and Procurement Canada • IT Security Risk Management: A Lifecycle Approach, Canadian Centre for Cyber Security • The 18 CIS Critical Security Controls, Center for Internet Security • COBIT 2019 Framework (Control Objectives for Information and Related Technology), Information Systems Audit and Control Association • ISO/IEC 27001, Information Security Management, International Organization for Standardization

Criteria	Sources
Communications Security Establishment Canada and the Canadian Centre for Cyber Security conduct security assessments of cloud service providers and communicate the results to federal departments.	• *Communications Security Establishment Act* • Policy on Government Security, Treasury Board • Directive on Security Management, Treasury Board • Policy on Service and Digital, Treasury Board • Directive on Service and Digital, Treasury Board • Cloud Service Provider Information Technology Security Assessment Process, Canadian Centre for Cyber Security • Guidance on the Security Categorization of Cloud-Based Services, Canadian Centre for Cyber Security • IT Security Risk Management: A Lifecycle Approach Canadian Centre for Cyber Security • Government of Canada Cloud Operationalization Framework, Treasury Board of Canada Secretariat • The 18 CIS Critical Security Controls, Center for Internet Security • COBIT 2019 Framework (Control Objectives for Information and Related Technology), Information Systems Audit and Control Association • ISO/IEC 27001, Information Security Management, International Organization for Standardization

Criteria	Sources
The Treasury Board of Canada Secretariat and Communications Security Establishment Canada (and its Canadian Centre for Cyber Security) have a process in place to liaise with stakeholders and deputy heads on security events that could have government-wide impacts. Selected departments document security event management practices and conduct exercises to detect, respond to, and report on cybersecurity events. They coordinate these activities within their departments, with cloud service providers, and with the Treasury Board of Canada Secretariat, Communications Security Establishment Canada, and the Canadian Centre for Cyber Security for government-wide events. The Treasury Board of Canada Secretariat coordinates government-wide security event management exercises to detect, respond to, and report on cybersecurity events.	• Policy on Government Security, Treasury Board • Directive on Security Management, Treasury Board • Policy on Service and Digital, Treasury Board • Directive on Service and Digital, Treasury Board • Government of Canada Cloud Operationalization Framework, Treasury Board of Canada Secretariat • Government of Canada Digital Standards: Playbook, Treasury Board of Canada Secretariat • Government of Canada Cyber Security Event Management Plan, Treasury Board of Canada Secretariat, 2019 • Event Logging Strategy, Government of Canada, 2019 • Event Logging Guidance, Treasury Board of Canada Secretariat • IT Security Risk Management: A Lifecycle Approach, Canadian Centre for Cyber Security • The 18 CIS Critical Security Controls, Center for Internet Security • Top 10 IT Security Actions, Canadian Centre for Cyber Security • Cloud Controls Matrix, Cloud Security Alliance • COBIT 2019 Framework (Control Objectives for Information and Related Technology), Information Systems Audit and Control Association

Criteria	Sources
The federal government is meeting its commitments to the environment and sustainable development in its procurement of cloud services.	• Policy on Green Procurement, Treasury Board • Contracting Policy, Treasury Board • Achieving a Sustainable Future: A Federal Sustainable Development Strategy for Canada 2016–2019, Environment and Climate Change Canada • Greening Government Strategy: A Government of Canada Directive, Treasury Board of Canada Secretariat, 2020 • Directive on the Management of Procurement, Treasury Board • Supply Manual, Public Services and Procurement Canada • Standard Acquisition Clauses and Conditions Manual, Public Services and Procurement Canada • Supply Manual, Shared Services Canada

Period covered by the audit

The audit covered the period from 1 April 2017 to 31 March 2022. This is the period to which the audit conclusion applies.

Date of the report

We obtained sufficient and appropriate audit evidence on which to base our conclusion on 21 October 2022, in Ottawa, Canada.

Audit team

This audit was completed by a multidisciplinary team from across the Office of the Auditor General of Canada led by Jean Goulet, Principal. The principal has overall responsibility for audit quality, including conducting the audit in accordance with professional standards, applicable legal and regulatory requirements, and the office's policies and system of quality management.

Recommendations and Responses

In the following table, the paragraph number preceding the recommendation indicates the location of the recommendation in the report.

Recommendation	Response
7.31 In consultation with Shared Services Canada and Public Services and Procurement Canada, the Treasury Board of Canada Secretariat should do the following: • Extend the requirement for guardrails to cloud service provider contracts that stem from supply arrangements established by Public Services and Procurement Canada. • Clarify who is responsible for the initial validation and ongoing monitoring of cloud guardrail controls and what processes they should follow.	**The Treasury Board of Canada Secretariat's response.** Agreed. The Treasury Board of Canada Secretariat will work with Shared Services Canada, Communications Security Establishment Canada, and Public Services and Procurement Canada to • publish the existing, approved Cloud Responsibility Matrix to formally identify who is responsible for validating, ongoing monitoring, performing oversight and compliance of the cloud guardrail controls by end of September 2022 • clarify and extend the processes to be followed for cloud service provider contracts awarded by Public Services and Procurement Canada as part of the updates to the Standard Operating Procedure for Validating Cloud Guardrails by December 2022 • update the GC Cloud Guardrails and the Directive on Service and Digital to reflect guardrail controls that apply to cloud services including cloud services procured by Public Services and Procurement Canada by January 2023 In addition, the Treasury Board of Canada Secretariat will • establish a score card to report on departments' level of adherence to the GC Cloud Guardrails by February 2023 • collaborate with Shared Services Canada in their efforts to implement tools to automate guardrail monitoring for cloud service providers in the Government of Canada by April 2023 • continue to provide advice and guidance to departments on ensuring that they perform security assessment and authorization activities for cloud-based applications using tools such as the Security Playbook for Information System Solutions, which outlines a set of security tasks for consideration when designing and implementing solutions for Government of Canada information systems in cloud environments

Recommendation	Response
7.40 The Treasury Board of Canada Secretariat should do the following: • Ensure that the Government of Canada Cyber Security Event Management Plan applies to the evolving cloud environment and shared responsibilities, review and test it at least annually, and update it as needed. • Follow up annually to ensure that departments finalize, implement, and regularly test their security event management plans.	**The Treasury Board of Canada Secretariat's response.** Agreed. The Treasury Board of Canada Secretariat will ensure that • the Government of Canada Cyber Security Event Management Plan is reviewed and tested at least annually and updated as appropriate. This includes an update to the plan, which is targeted for publication by late fall 2022, and inclusion of cloud-based scenarios in the plan's simulation exercises • a process is in place to validate that departments have established and implemented a departmental cyber security event management plan that aligns with the Government of Canada's plan and that the plans are submitted on an annual basis to the Treasury Board of Canada Secretariat for review by fall 2023 • tools are planned for and available which will enable departments to regularly test their departmental cyber security event management plan, such as a canned tabletop product that focuses on a cloud-based scenario that departments can leverage to run their own simulation exercise, as well as exploring options to establish a procurement vehicle that will enable facilitated cloud-based simulation exercises by March 2023
7.47 In consultation with Communications Security Establishment Canada, Shared Services Canada, Public Services and Procurement Canada, and departments, the Treasury Board of Canada Secretariat should document and proactively communicate to any department that is using or contemplating cloud services the roles and responsibilities needed to design, implement, validate, monitor, coordinate, and enforce the security controls needed to protect sensitive and personal information in the cloud. The secretariat should review and update these roles and responsibilities at least every 12 months.	**The Treasury Board of Canada Secretariat's response.** Agreed. The Treasury Board of Canada Secretariat will work with Communications Security Establishment Canada, Shared Services Canada, Public Services and Procurement Canada, and departments to • publish the existing approved Cloud Responsibility Matrix to formally identify who is responsible for validating, ongoing monitoring, performing oversight and compliance of the cloud guardrail controls by end of September 2022

Recommendation	Response
	• undertake a review to ensure that the roles and responsibilities required in support of the design, implementation, validation, monitoring, coordination, and enforcement of all the security controls needed to protect sensitive and personal information in the cloud are relevant, updated, and documented in the Cloud Responsibility Matrix by March 2023 • increase regular, proactive communications on roles and responsibilities to any department that is using or considering the use of cloud services by providing updates to the Cloud Responsibility Matrix through forums such as the Government of Canada Enterprise Architecture Review Board, Director General Cloud Steering Committee, Government of Canada Cloud and Computing Network of Expertise Working Group, and information sharing sites such as the Government of Canada Cloud InfoCentre beginning in September 2023 • establish a process for an annual review and publication of the Cloud Responsibility Matrix and providing updates to the community by March 2023
7.58 In consultation with Shared Services Canada and other departments, the Treasury Board of Canada Secretariat should do the following: • Develop and provide a costing model to help departments make informed decisions about moving to the cloud and determine whether additional resources and funding are required. • Help departments determine their long-term operational funding needs and support their access to funding so they can fulfill their evolving responsibilities for cloud operations, including securing sensitive information in the cloud.	**The Treasury Board of Canada Secretariat's response.** Agreed. The Treasury Board of Canada Secretariat is currently consulting with the Government of Canada community to discuss cloud operational models, prioritization criteria, and associated funding models. A series of recommendations will inform the Government of Canada Chief Information Officer on direction for operating in the cloud in fall 2022. The secretariat will, in consultation with departments and Shared Services Canada • develop and provide a costing model and guidance to help departments make informed decisions about moving to the cloud by June 2023 • assist departments including Shared Services Canada with forecasting medium- and long-term costs required to operate in a cloud environment by June 2023

Recommendation	Response
7.72 Public Services and Procurement Canada and Shared Services Canada should include environmental criteria when procuring cloud services to support sustainability in procurement practices and contribute to achieving Canada's net-zero goal.	**The departments' response.** Agreed. Public Services and Procurement Canada and Shared Services Canada agree that environmental criteria should be included in the procurement of cloud services. The Shared Services Canada Cloud Framework Agreement currently does not in itself include sustainability requirements; it does provide the ability to include such requirements in future solicitations. Shared Services Canada has developed rated environmental criteria, which it plans on including in upcoming competitive solicitations under the Government of Canada Cloud Framework Agreement beginning in fall 2022, which includes greening requirements related to greenhouse gas reduction targets. In addition, Shared Services Canada has confirmed that at this time 7 of the 8 Government of Canada Cloud Framework Agreement vendors have equal or enhanced targets compared with Canada's net-zero commitments. The Public Services and Procurement Canada software as a service supply arrangement does not evaluate environmental criteria; however, it does collect this information from suppliers in order to assist clients in evaluating the solutions available through the supply agreement. Public Services and Procurement Canada plans to update the environmental information collected in its software as a service supply agreement and plans to refresh the agreement in order to address Government of Canada priorities related to net-zero greenhouse gas emissions. The supply agreement will provide the ability for clients to include environmental criteria in bid solicitations issued against the agreement, and Public Services and Procurement Canada plans to develop resulting contract clauses regarding greenhouse gas emissions related to greenhouse gas reduction targets. Shared Services Canada and Public Services and Procurement Canada have also been working together to further align the approach to cloud procurement. As part of this exercise, a standard template for cloud contracts is being developed, which is anticipated to be released by fall 2022. This will include standard sustainability terms for cloud providers.