

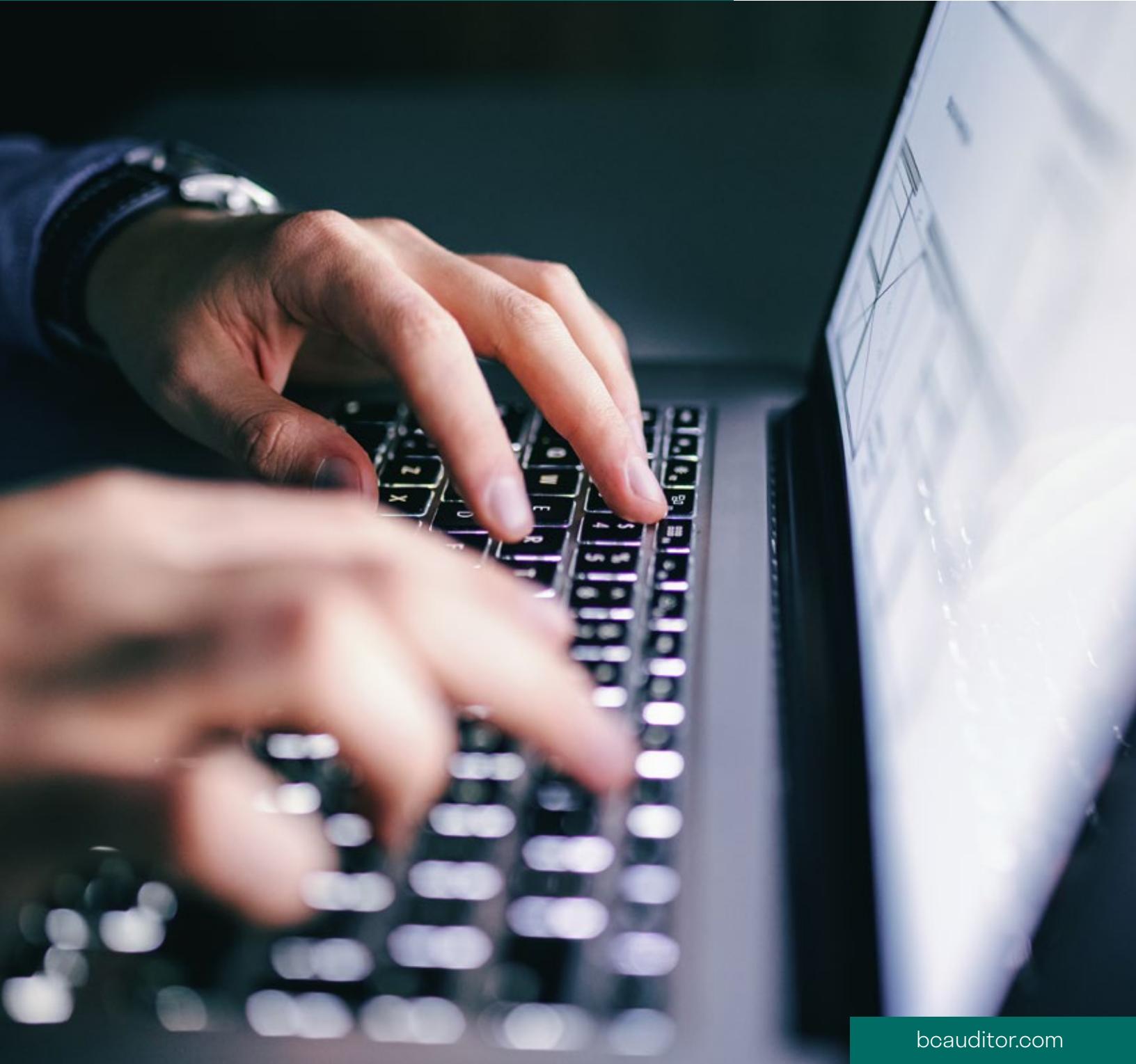


OFFICE OF THE
Auditor General
of British Columbia

IT ASSET MANAGEMENT IN B.C. GOVERNMENT

An independent audit report

November 2020



bc auditor.com

The Honourable Raj Chouhan
Speaker of the Legislative Assembly
Province of British Columbia
Parliament Buildings
Victoria, British Columbia
V8V 1X4

Dear Mr. Speaker:

I have the honour to transmit to the Speaker of the Legislative Assembly of British Columbia the report, *IT Asset Management in B.C. Government*.

We conducted this audit under the authority of section 11(8) of the *Auditor General Act*. 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*.



Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.
January 2021

CONTENTS

Report highlights	3
Auditor General's comments	4
Audit at a glance	7
Summary	9
Summary of recommendations	12
Response from the auditee	13
About the audit	15
Background	15
Audit scope	18
Audit method	19
Audit objective, criteria and conclusion	20
Key findings and recommendations	23
Defining and establishing cybersecurity roles and responsibilities throughout an organization	24
Maintaining inventories of IT assets	25
Maintaining maps of organizational communication and data flows	30
Prioritizing IT assets based on classification, criticality and business value	31
Audit quality assurance	33
Glossary	34
Appendix A: NIST cybersecurity framework core functions and categories	38
Appendix B: Criteria and bases of assessment validation	39

The Office of the Auditor General of British Columbia would like to acknowledge with respect that we conduct our work on Coast Salish territories. Primarily, this is on the Lkwungen-speaking people's (Esquimalt and Songhees) traditional lands, now known as Victoria, and the WSÁNEĆ people's (Pauquachin, Tsartlip, Tsawout, Tseycum) traditional lands, now known as Saanich.

REPORT HIGHLIGHTS

We selected five B.C. government ministries and looked to see whether they have managed their IT assets in accordance with good cybersecurity practices.



 We concluded that, overall, the selected ministries **HAVE NOT MANAGED IT ASSETS IN ACCORDANCE WITH GOOD PRACTICES**, with the exception of one ministry and related organization.

 We found **GAPS IN POLICIES AND GUIDANCE, AND IN INVENTORY MANAGEMENT**.

 These gaps could hinder the ministries' ability to develop and implement appropriate safeguards to protect IT assets from cybersecurity threats.



We made seven recommendations to help government improve the management of its IT assets for cybersecurity.



About IT asset management and cybersecurity



Cybersecurity incidents are increasing in frequency worldwide.



The government of B.C. relies heavily on the use of technologies to deliver services and programs.



An effective cybersecurity program starts with solid IT asset management.

Organizations can't protect what they don't know they have.



AUDITOR GENERAL'S COMMENTS

MICHAEL A. PICKUP, FCPA, FCA
Auditor General of British Columbia

“Cybercrime is the most common cyber threat that Canadians and Canadian organizations are likely to encounter.”—Canadian Centre for Cyber Security, National Cyber Threat Assessment 2018

More and more often, we hear about data breaches through cyberattacks. A cyberattack is a deliberate exploitation of computer systems, technology-dependent enterprises, and networks. Organizations with poorly managed security for systems and infrastructure, and poor cybersecurity practices, are vulnerable to cyberattacks. Studies show that:

- 70% of breaches are perpetrated by external actors¹
- hackers attack every 39 seconds, or an average of 2,244 times per day²
- data breaches exposed 8.4 billion records globally in the first quarter of 2020³

As noted in our recent report *Detection and Response to Cybersecurity Threats on BC Hydro's Industrial Control Systems*, “cybersecurity is no longer defined by the prevention of attacks—attackers will eventually succeed. Instead, cybersecurity is defined by how quickly an organization can detect, and respond to, an attack.”

Many good practices are available for mitigating the risk of cyber threats. A strong IT asset management system is the foundation for a robust cybersecurity management program. Simply put, organizations can't protect what they don't know they have. It is critical that organizations have all the details about the applications and devices being used, according to prescribed policies and standards, and clearly established roles and responsibilities for cybersecurity, including those pertaining to service providers and vendors.

¹ Verizon 2020 Data Breach Investigations Report

² University of Maryland Clark School of Engineering Study

³ RiskBased Security 2020 Q1 Report: Data Breach QuickView

The COVID-19 pandemic has caused the Government of British Columbia to take measures to slow the spread of the coronavirus and keep employees safe and healthy. For example, telework arrangements for employees and contractors, collaboration tools and web-based applications have been adopted to provide services for citizens.

Recent research shows that measures like these can elevate the risk to cybersecurity in every aspect of business operation. Since remote networks now need to be publicly accessible, their once well-defined boundaries are now blurred, making existing controls ineffective or unavailable. Information technology (IT) leaders are facing many new challenges, providing users with the access they need while meeting security needs in a complex IT environment.

About this audit

In this audit, we selected five ministries (see [Exhibit 2](#)) and examined how they are managing their IT assets in the context of establishing a robust cybersecurity management program. We selected these ministries because they provide essential services to British Columbians, and their corresponding sectors represent 89% of total core government IT capital spending.

What we found

We concluded that, overall, the selected ministries have not managed IT assets in accordance with good practices, with the exception of one ministry and related organization. This could hinder the ministries' ability to develop and implement appropriate safeguards to protect their IT assets from cybersecurity threats.

We provided seven recommendations to help the selected ministries and related organizations improve their IT asset management practices in the context of cybersecurity. All of these recommendations have been accepted by the government.

For more information, see [Audit at a Glance](#).

Looking ahead

After reading this report, you may wish to ask the Office of the Chief Information Officer (OCIO) and all other ministries and related organizations the following questions:

1. How does the government keep its cybersecurity program up to date, and how will it match up with current good practices going forward?
2. How will the government test its cybersecurity program for effectiveness and responsiveness as it makes changes and the world continually evolves?

3. How has the government adjusted its cybersecurity program to ensure that it is effective against potentially increasing cyber threats during the ongoing COVID-19 pandemic?

Acknowledgements

I would like to thank everyone at the selected ministries and the Office of the Chief Information Officer for their co-operation and support during this audit.



Michael A. Pickup, FCPA, FCA
Auditor General of British Columbia
Victoria, B.C.
November 2020

AUDIT AT A GLANCE

Why we did this audit

Managing cybersecurity risk begins with managing IT assets. As the B.C. government uses more technologies to deliver services and programs, strong cybersecurity risk management becomes even more important.

Both the ministries and the private sector have seen more cybersecurity incidents, with real impacts for real people.

Purpose of our audit

To determine whether the five ministries (Citizens' Services, Finance, Health, Natural Resources, and Education) are effectively managing their IT assets in line with good practices as they work to protect government from cybersecurity threats.

Overall audit conclusion

The Office of the Chief Information Officer, Enterprise Services (OCIO-ES; part of the Ministry of Citizens' Services) and the Ministry of Education managed IT assets in accordance with good cybersecurity practices, with minor exceptions. Overall, they did what was reasonably expected.

The following ministries did not manage IT assets in accordance with good cybersecurity practices, as they did not manage risks as expected:

- Ministry of Citizens' Services, with the exception of OCIO-ES
- Ministry of Finance and related agencies (the BC Public Service Agency, and Government Communications and Public Engagement)
- Ministry of Health
- the natural resource ministries

The weakness in their practices could hinder their ability to protect their IT assets from cybersecurity threats.

We made seven recommendations to government on how to improve the management of IT assets, and all were accepted.

What we found

Cybersecurity roles and responsibilities not well managed

Roles and responsibilities not clearly defined for employees and third parties

- Security standards lacked specific definitions of roles and responsibilities
- Organizational charts, job descriptions, service agreements and contracts did not address cybersecurity roles and responsibilities

RECOMMENDATION 1

IT asset inventories not appropriately maintained

Poor guidance on creating reliable IT inventory records

Policies and security standards lacked guidance on:

- which tools and methods to use
- what information is essential for inventorying IT assets
- prioritizing IT assets to manage cybersecurity risks

Ministries did not consistently manage IT asset inventories

- Central asset registry not fully used
- Some tools designed for financial purposes, not cybersecurity
- Lack of consistency in reporting
- Varied approaches and tools made it difficult to ensure completeness and accuracy of inventories

Inventories were incomplete and inaccurate

- Not all devices included (e.g., VoIP phones)
- Software platforms and applications not in central asset registry
- Third-party systems not identified or tracked
- Records missing important data (e.g., name and location)

Ministries did not periodically review IT asset inventories

- No formal processes, tools, records
- Lacked processes or systems to auto-detect:
 - unauthorized devices on the network
 - unauthorized applications downloaded
 - unauthorized information systems hosted by third parties

RECOMMENDATION 2

RECOMMENDATION 3

RECOMMENDATION 4

RECOMMENDATION 5

Maps of communication and data flows not kept as required

Maps lacked key data and were inaccurate, incomplete and outdated

- Not all organizations maintained maps
- Existing maps inconsistent and missing important data
- No evidence of periodic reviews
- Responsibility for maintaining maps unclear

IT assets not appropriately prioritized

Inventories were missing classification, criticality, and business value data

- IT asset inventory documents lacked key information (except central asset registry)
- IT assets not prioritized for cybersecurity purposes

RECOMMENDATION 6

RECOMMENDATION 7

SUMMARY

Managing IT assets is the foundation for building a strong cybersecurity program

The Government of British Columbia uses computer systems, the internet, wireless networks and smart devices to deliver programs efficiently. While highly beneficial, this comes with risks. Exploitation of vulnerabilities by attackers, technology failures and insider mistakes could each result in government being unable to provide key services or to prevent unauthorized access to sensitive information, such as personal health information, identity or banking information.

The National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS) have developed frameworks to help organizations develop strong cybersecurity programs for managing the risks of cyberattacks. Cybersecurity is the protection of information assets by addressing threats to information processed, stored and transported by networked information systems.

According to the NIST and CIS cybersecurity frameworks, identifying and managing information technology (IT) assets is the foundation for effective cybersecurity risk management. Organizations cannot protect, monitor or respond quickly to cybersecurity incidents involving things they do not know they have.

Good practices in IT asset management involve identifying, tracking and prioritizing devices and systems, and monitoring asset records regularly

Based on the NIST and CIS cybersecurity frameworks, managing IT assets encompasses the following good practices:

- identifying, tracking and prioritizing devices, systems running these devices, and applications used by staff on these devices, whether located internally or externally
- monitoring asset records, sometimes known as asset inventories, to ensure they are accurate, complete and current
- maintaining maps that show interconnections between devices, systems and applications, and flows of key data
- defining and establishing cybersecurity roles and responsibilities for the entire organization, including third-party stakeholders

Through the Office of the Government Chief Information Officer (OCIO), the B.C. government has established policies regarding the protection of information and technology assets. These policies require ministries to identify assets under their control and document, maintain and verify asset inventories regularly.

Our audit examined whether the following selected B.C. government ministries are managing IT assets they are responsible for, consistent with good practices in IT asset management for cybersecurity purposes:

- Ministry of Citizens' Services
- Ministry of Finance
- Ministry of Health
- the natural resource ministries
- Ministry of Education

We conducted our fieldwork between December 2017 and June 2019. We focused on the OCIO's responsibilities and the agencies, divisions and/or branches within five selected ministries (21 lines of business; see [Exhibit 2](#)). We selected these ministries because they provide essential services to British Columbians, and their corresponding sectors represent 89% of the total core government IT capital spending.

Four of the selected B.C. ministries have not managed IT assets in accordance with good practices

We concluded that OCIO Enterprise Services (OCIO-ES; part of the Ministry of Citizens' Services) and the Ministry of Education managed IT assets in accordance with good practices that provide the foundation for building strong defences against cybersecurity threats, with exceptions. However, the following ministries and related organizations did not manage IT assets in accordance with good cybersecurity practices:

- Ministry of Citizens' Services (with the exception of OCIO-ES)
- Ministry of Finance and related agencies (the BC Public Service Agency, and Government Communications and Public Engagement)
- Ministry of Health
- the natural resource ministries

We found that the government's *Core Policy and Procedures Manual* and the OCIO's Information Security Standard lacked specific guidelines for identifying and managing

IT assets for the purpose of managing cybersecurity risks. Also, we found that roles and responsibilities for maintaining IT asset inventories and cybersecurity were not clearly established within the ministries and between the OCIO and the ministries.

In addition, we found that the selected ministries' IT asset inventories and maps of organizational communication and data flows were not accurate, complete and current:

- not all IT assets were identified and tracked, and those that were identified were not tracked consistently within or among the selected ministries
- IT asset inventories and communication and data flow diagrams lacked some key information, including classification, criticality and business value information
- not all inventories of IT assets and communication and data flow maps were monitored to ensure that they were accurate, complete and current

These foundational deficiencies could hinder the ministries' ability to develop and implement subsequent safeguards for protecting their IT assets from cybersecurity threats.

SUMMARY OF RECOMMENDATIONS

We recommend that the Office of the Chief Information Officer, ministries and, when applicable, third-party providers:

- 1** Work together to identify, establish and document cybersecurity roles and responsibilities for employees and for third-party stakeholders, including where those persons have a role in managing IT assets.

We recommend that the Office of the Chief Information Officer and the ministries:

- 2** Collaborate to review and update core government policies and standards and ministry-specific guidelines in accordance with good cybersecurity practices regarding IT asset inventories.
- 3** Collaborate to adopt a consistent approach for identifying and tracking their IT assets to ensure the completeness and accuracy of inventories of IT assets.
- 4** Collaborate to ensure that inventories are complete and accurate, based on the assets' risk and the ministries' risk appetite.
- 5** Collaborate to establish formal periodic reviews and/or adopt an automated tool for ensuring that records of IT assets are kept accurate, complete and current.
- 6** Collaborate to develop specific guidelines and procedures for ensuring that maps of key organizational communication and data flows include key information and are kept accurate, complete and current.
- 7** Collaborate to ensure that IT asset inventory records meet the expectations established in government standards and guidelines for classification, criticality and business value information based on risk assessments.

RESPONSE FROM THE AUDITEE

The Province thanks the Office of the Auditor General (OAG) for the analysis and valuable recommendations in the Information Technology (IT) Asset Management report, recently completed by your office. This timely report has provided valuable feedback to inform our efforts to keep pace with the ever changing and increasing security threats that all organizations face. I appreciate the Office of the Auditor General (OAG) acknowledging the good work we are doing and also in helping to validate government's current course of action to increase security in the area of asset management. The Province accepts all 7 recommendations in the report.

The protection of government and citizen information is of primary importance and IT assets often hold information deemed to be sensitive. While government has security controls to protect IT assets and the information residing on them there is more we can do in this area. Existing controls include device authentication, encryption, ability to remotely wipe a device that is lost or stolen, and regular patching of vulnerabilities.

The Office of the Chief Information Officer (OCIO) will work with ministries to conduct a review of cybersecurity roles and responsibilities and ensure key roles are understood. We will review and update core government policies and standards in accordance with current cybersecurity framework and practices on inventory of IT assets. The OCIO is continuing efforts to improve the handling of IT assets to include recent launch of a data framework to provide a common approach to assets such as workstations, a Workstation Fleet Management Dashboard based on the data framework to provide ministries access to current information about their assets, proactive monitoring, and enhanced inventory management. Relevant assets provided to employees will be captured within this system and the introduction of this new service and associated processes will enable government to meet recommendations to adopt a consistent approach for identifying and tracking relevant information about their IT assets to increase the completeness and accuracy of the inventory. The OCIO will ensure processes are in place to ensure the records of relevant IT assets are complete, accurate, and current.

The OCIO and ministries will work to develop guidelines and procedures for maintaining maps of key communication and data flows for systems that are risk-based. OCIO will work with third party-providers to ensure they benefit from this work and are following similar practices with respect to strong IT asset management practices.

These policy and process improvements will be completed by December 2021. The Province accepts the valuable recommendations of the Office of the Auditor General which will improve the government asset management strategy, the information security program, and the protection of sensitive information.

ABOUT THE AUDIT

Background

Technical terms used in the report are defined in a [Glossary on page 34](#)

The Government of British Columbia uses computer systems, the internet, wireless networks and smart devices to deliver programs efficiently. While highly beneficial, this comes with risks. Computer security incidents, such as exploitation of vulnerabilities by attackers, technology failures and insider mistakes, could result in government being unable to provide key services or to prevent unauthorized access to sensitive information, such as personal health information, identity or banking information.

What is cybersecurity and why is it important?

Cybersecurity is the protection of information assets by addressing threats to information processed, stored and transported by networked information systems. It includes technologies, processes and controls designed to protect assets such as computers, networks, applications, devices and data. Effective cybersecurity reduces the likelihood of attackers causing harm by exploiting weaknesses in systems, networks and technologies.

Cybersecurity is the protection of information assets by addressing threats to information processed, stored and transported by networked information systems.

In recent years, media reports have indicated that cybersecurity incidents are increasing in both frequency and impact on organizations and individuals. Service disruptions, financial loss, breach of personally identifiable information and loss of stakeholder confidence are all possible outcomes. As cyberattacks grow in frequency and sophistication, organizations are realizing that this is a critical risk to address.

How does an organization appropriately manage cybersecurity risk?

The first step in appropriately managing cybersecurity risk is for an organization to identify and manage its information technology (IT) assets in accordance with their relative importance to business objectives and strategy. According to the National Institute

of Standards and Technology (NIST) and the Center for Internet Security (CIS), which set standards for information technology and cybersecurity, managing IT assets is the foundation for effective cybersecurity risk management, and this is the primary focus of our audit. (See [Appendix A](#) for the NIST cybersecurity framework core functions and categories.)

IT assets are the data, personnel, devices, systems and facilities that enable an organization to achieve its business objectives. They must be identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.

Organizations cannot protect the things they don't know they have.

The basic message of the NIST and CIS guidance is that *organizations cannot protect the things they don't know they have*. Knowing what IT-related assets an organization has (and who owns them) and categorizing those assets is essential in protecting against cybersecurity threats. An organization cannot protect everything equally, but it should find a way to identify and control those assets that matter.

What is the B.C. government currently doing to manage IT assets?

Core government policies

The B.C. government has established core policies to support the carrying out of its service objectives, contribute to effective management and assist staff in making sound decisions. Chapters 8 and 12 of the *Core Policy and Procedures Manual* outline the overall responsibilities and requirements for the management of assets:

- Chapter 8, Asset Management, mandates that each government organization is responsible for the administration, control, proper accounting and safeguarding of government assets coming under its custody or control.
- Chapter 12, Information Management and Information Technology Management, states that information management is a core component of government infrastructure and is the intellectual capital of responsible governance. This policy places the responsibilities for the corporate management of information and IT on the government chief information officer (GCIO).

In the B.C. government, the Office of the Chief Information Officer (OCIO) operates within the Ministry of Citizens' Services and leads the development of strategy, policy and standards for telecommunications, information technology, IT security and a variety of other IT initiatives.

The GCIO is the senior executive of the OCIO and is responsible for ensuring that the security of government's information is maintained and protected. The GCIO is responsible for governance authority for standards setting, oversight and approvals for government organizations' information and communications technology. The GCIO develops, proposes and maintains government-wide information management/information technology policy, procedures and standards, and evaluates compliance.

Chapter 2 of the government's Information Security Policy, developed by the OCIO, focuses on management of information systems and devices. The OCIO also developed the Information Security Standard, which provides the framework, in alignment with the Information Security Policy, within which government organizations meet their goals for protecting government information and technology assets. Chapter 4 of the Information Security Standard establishes the blueprint for protection: what assets to protect, who protects them and how much protection is adequate. Specifically, the policy requires that:

- information owners identify assets under their control
- information owners and information custodians⁴ document, maintain and verify asset inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of a risk management strategy

In addition, the OCIO developed a strategy guide, *Defensible Security for Public Sector Organizations*, for public sector organizations to use in applying appropriate safeguards and maintaining a defensible level of security. This is a good starting place for organizations to determine their cybersecurity posture and identify areas where improvement is required. The guide notes that one key to success is to identify critical systems and data that are important to the organization.

The ministries' past annual information security reviews (a self-assessment reported to the OCIO) also indicated that IT asset management is a key concern in government.

⁴ According to the Information Security Standard (September 2019), information owners have the responsibility and decision-making authority for information throughout its lifecycle, including creating, classifying, restricting, regulating and administering its use or disclosure. Information custodians maintain or administer information resource on behalf of the information owner. Custodianship includes responsibility for accessing, managing, maintaining, preserving, disposing and providing security for the information resource. Information custody means having physical possession of information without necessarily having responsibility for the information.

Ministry responsibilities

Ministries are expected to comply with core policies, standards and guidelines established by the OCIO. Each ministry, through its chief information officer, is required to reinforce information management and information technology (IM/IT) services from a risk management perspective and ensure compliance with the IM/IT policies and standards. Ministry chief information officers are responsible for aligning their policies and procedures with the related government policies, standards and guidelines.

Audit scope

This is an audit to determine whether the following selected B.C. government ministries are managing IT assets they are responsible for, consistent with good practices, as the first step in building strong defences against cybersecurity threats:

- Ministry of Citizens' Services
- Ministry of Finance
- Ministry of Health
- the natural resource ministries
- Ministry of Education

We conducted our field work between December 2017 and June 2019. We focused on the responsibilities of the Office of the Chief Information Officer and the agencies, divisions and/or branches within five selected ministries (21 lines of businesses in total; see Exhibit 1). We selected these ministries because they provide essential services to British Columbians, and their corresponding sectors represent 89% of the total core government IT capital spending.

EXHIBIT 1: The selected ministries and related organizations

Ministry	Lines of business	Lines of business assessed
Citizens' Services	7	<p>Lines of business (combined assessment for the following branches):</p> <ul style="list-style-type: none"> ▪ Information Management Branch ▪ Service BC ▪ Queen's Printer ▪ BC Mail Plus <p>OCIO Enterprise Services Division (combined assessment for the following branches):</p> <ul style="list-style-type: none"> ▪ Device Services ▪ Hosting Services ▪ Network Communications and Collaboration Services

Ministry	Lines of business	Lines of business assessed
Finance	6	<p>Lines of business (combined assessment for the following branches):</p> <ul style="list-style-type: none"> ▪ Information Management Branch ▪ Corporate Accounting Services ▪ Provincial Treasury ▪ Financial Institutions Commission (Note 1) <p>Government Communications and Public Engagement (Note 2)</p> <p>BC Public Service Agency</p>
Health	6	<p>Lines of business (combined assessment for the following branches):</p> <ul style="list-style-type: none"> ▪ IT Services Branch ▪ Business Management Office ▪ Health Information Privacy, Security and Legislation ▪ Data Management Stewardships ▪ Vital Statistics Agency ▪ HealthLink BC
Natural resource ministries	1	Information, Innovation and Technology Division (Note 3)
Education	1	Services and Technology
Total	21	

Notes:

1. The Financial Institutions Commission became a Crown entity as of November 1, 2019, and is now called the BC Financial Services Authority.
2. Effective July 11, 2019, the Government Digital Experience Division became part of the Ministry of Citizens' Services and continues its day-to-day relationship with Government Communications and Public Engagement.
3. This division supports all of the natural resource ministries and is now under the Ministry of Environment and Climate Change Strategy. The natural resource ministries include Agriculture; Energy, Mines and Petroleum Resource; Environment and Climate Change Strategy; Forests, Lands, Natural Resource Operations and Rural Development; and Indigenous Relations and Reconciliation.

Audit method

The report is dated November 22, 2020. This is the date on which the audit team finished gathering the evidence used to determine the findings and conclusion of the report.

We developed a set of questionnaires based on the NIST Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0; see [Appendix A](#)) and ISACA's⁵ audit/assurance program *Cybersecurity: Based on the NIST Cybersecurity Framework*. We also cross-referenced our questionnaires with the government's *Core Policy and Procedures Manual* and

⁵ ISACA, previously known as the Information Systems Audit and Control Association, is an independent, non-profit, global association that engages in the development, adoption and use of globally accepted, industry-leading knowledge and practices for information systems. (Source: <https://www.isaca.org>)

Information Security Standard for consistency. We sent the questionnaires to each of the five selected ministries and their related organizations and asked them to assess whether they are managing IT assets in accordance with good practices and to provide supporting documents. The questionnaires were completed with input from staff working in the 21 lines of business listed in [Exhibit 1](#).

We validated the self-assessment results through:

- examination of supporting documents, which included policies, documented procedures, lists of IT assets, network and data flow diagrams, organizational charts and relevant contracts
- interviews and email exchanges with key personnel charged with IT asset management at the five selected ministries and related organizations

Audit objective, criteria and conclusion

Audit objective

Our overall audit objective was to determine whether selected B.C. government ministries have managed IT assets in accordance with good cybersecurity practices that provide the foundation for building strong defences against cybersecurity threats.

Audit criteria

We examined whether the five selected ministries and their related organizations had:

1. maintained an inventory of physical devices and systems under ministries' responsibility
2. maintained an inventory of software platforms and applications under ministries' responsibility
3. maintained maps of organizational communication and data flows
4. maintained an inventory of information systems used in business operations and hosted or owned by third parties
5. prioritized IT assets under their responsibility based on classification, criticality and business value
6. defined and established cybersecurity roles and responsibilities for ministries' entire workforce and third-party stakeholders (e.g., suppliers, customers, partners)

See [Appendix B](#) for details on how we assessed each criterion.

Audit conclusion

We concluded that the OCIO-ES (part of the Ministry of Citizens' Services) and the Ministry of Education managed IT assets in accordance with good practices that provide the foundation for building strong defences against cybersecurity threats, with exceptions. However, the following ministries and related organizations did not manage IT assets in accordance with these cybersecurity practices:

- Ministry of Citizens' Services
- Ministry of Finance (including the BC Public Service Agency and Government Communications and Public Engagement)
- Ministry of Health
- the natural resource ministries

We found that the established policies and standards for IT asset management lacked specific guidelines for identifying and managing IT assets for the purpose of managing cybersecurity risks. Also, we found that roles and responsibilities for maintaining IT asset inventories and cybersecurity were not clearly established either within ministries or between the Office of the Chief Information Officer and the ministries.

In addition, we found that the selected ministries have inventories of IT assets and maps of organizational communication and data flows. However, they were not complete and accurate because:

- not all IT assets were identified, consistently tracked and monitored
- information important for managing cybersecurity was missing, including classification, criticality and business value

These foundational deficiencies could hinder the ministries' ability to develop and implement safeguards for protecting their IT assets from cybersecurity threats.

Subsequent events

Over the last months of our field work, the novel coronavirus (COVID-19) increased the risk of cybersecurity threats.

The World Health Organization declared the COVID-19 outbreak a Public Health Emergency of International Concern on March 11, 2020. The pandemic has required organizations

and individuals to embrace new practices, such as remote working/learning and physical distancing in public places.

The B.C. government's IM/IT resources are focused on providing uninterrupted services through remote working/services arrangements. To get their work done remotely, teleworking employees need to access government data over remote network connections, using specialized teleworking tools to handle information and maybe using non-government-issued computers to conduct government businesses. Remote networks necessarily need to be publicly accessible, and the once well-defined network boundaries—where strong cybersecurity controls could be implemented—are less defined. Managing network security is more difficult because monitoring devices are not readily accessible, and vulnerable personal communications channels may be turned on by employees. Meanwhile, cybercriminals are using COVID-19 as bait, impersonating trusted brands to mislead employees and business users into downloading malicious computer programs, such as ransomware, disguised as legitimate applications.

IT professionals within government are relying on properly installed technology, such as virtual private network servers, logon credential checking, web application security, anti-malware solutions, encryption of data—in storage and in transmission—to protect against cybersecurity threats. As such, a well-maintained inventory record of IT assets will be essential to help IT professionals identify what they have and take necessary steps to secure those devices and applications.

The impact of the COVID-19 pandemic on the ministries' ability to manage IT assets, using remote working arrangements, was not within the scope of this audit.

KEY FINDINGS AND RECOMMENDATIONS

Exhibit 2 is a summary of the overall audit results for selected ministries and related organizations by audit criteria. The table summarizes how well each of the selected ministries and related organizations had identified and managed their information technology (IT) assets to mitigate cybersecurity risks.

Exhibit 2 shows that the Ministry of Education and the Office of the Chief Information Officer (OCIO) Enterprise Services Division of the Ministry of Citizens' Services had implemented good IT asset management practices on five of the six criteria. The other four ministries and related organizations did not manage their IT assets in accordance with good cybersecurity practices. A detailed explanation of the deficiencies found under each of the criteria follows.

EXHIBIT 2: Summary of the audit results for selected ministries and related organizations by audit criteria

Audit criteria (Note 1)	Ministry of Citizens' Services		Ministry of Finance			Ministry of Health	Natural resource ministries	Ministry of Education
	Lines of business (Note 2)	OCIO Enterprise Services (Note 3)	Lines of business (Note 4)	BC Public Service Agency	Government Communications and Public Engagement	Lines of business (Note 5)	Line of business (Note 6)	Line of business
1) Ministry has maintained an inventory of physical devices and systems under their responsibility	No	Yes, with exceptions	No	No	No	No	No	Yes, with exceptions
2) Ministry has maintained an inventory of software platforms and applications under their responsibility	No	No	No	No	No	No	No	Yes, with exceptions
3) Ministry has maintained maps of organizational communication and data flows	No	Yes, with exceptions	Yes, with exceptions	No	No	Yes, with exceptions	No	Yes, with exceptions
4) Ministry has maintained an inventory of information systems used in business operations and hosted or owned by third parties	No	Yes, with exceptions	No	No	No	No	No	Yes, with exceptions
5) Ministry has prioritized IT assets under their responsibility based on classification, criticality and business value	No	N/A	No	No	No	No	No	No
6) Ministry has defined and established cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners)	Yes, with exceptions	Yes, with exceptions	Yes, with exceptions	Yes, with exceptions	Yes, with exceptions	Yes, with exceptions	Yes, with exceptions	Yes, with exceptions

Note 1: Conclusions against criteria—definitions:

Yes: criteria met

Yes, with exceptions: criteria met with exceptions

No: criteria not met

N/A: no third-party hosting services

Note 2: Ministry of Citizens' Services lines of business include Information Management Branch, Service BC, Queen's Printer and BC Mail Plus.

Note 3: OCIO Enterprise Services (OCIO-ES) includes Device Services, Hosting Services, and Network Communications and Collaboration Services.

Note 4: Ministry of Finance lines of business include Information Management Branch, Corporate Accounting Services, Provincial Treasury and Financial Institutions Commission.

Note 5: Ministry of Health lines of business include IT Services Branch, Business Management Office, Health Information Privacy, Security and Legislation Branch, Data Management Stewardships Branch, HealthLink BC and Vital Statistics Agency.

Note 6: Management of IT assets within the natural resource ministries is the responsibility of the Information, Innovation and Technology Division, which reports to the deputy minister, Ministry of Environment and Climate Change Strategy.

Defining and establishing cybersecurity roles and responsibilities throughout an organization⁶

Effective management of cybersecurity risks requires a clear understanding of the relationship between cybersecurity risks and organizational objectives. It should be part of the organizational culture and thus requires clearly defined and established cybersecurity roles and responsibilities for the entire workforce (e.g., governance, privacy, legal, strategic planning, IT investment management, project management, program management, analysts/specialists), including third-party stakeholders (e.g., suppliers, customers, partners).

Cybersecurity roles and responsibilities were not clearly defined or established for the entire workforce and third-party stakeholders

Responsibility for the Government of British Columbia's IT service is shared, with some central authority and some authority distributed among the ministries. OCIO Enterprise Services (OCIO-ES) is a central government division within the Ministry of Citizens' Services that provides device, hosting and network services to all organizations across the provincial government. The shared model affects the roles and responsibilities of those providing the service. We looked to see whether ministries were clear about their roles and responsibilities in identifying and managing IT assets.

During the audit we found that there was confusion, both between the ministries and OCIO-ES, and between organizations within each ministry, about who was responsible for maintaining IT asset inventory records. Staff at some ministries indicated that they expected their ministry's information management branch to track IT assets, and staff at other

⁶ See [Exhibit 2](#), Criterion 6

ministries assumed that it is the OCIO's responsibility. As a result, those ministries did not identify or track some of their IT assets.

We also looked to see if the selected ministries' security policies, organization charts, job descriptions, agreements, RACI charts, service-level agreements and contracts specifically include cybersecurity roles and responsibilities (see [Appendix B](#), criterion 6).

RACI: Responsible, Accountable, Consulted, Informed. Each letter of this word represents a task.

We found that:

- The OCIO's Information Security Standard provides guidance on what information assets to protect, who protects them and how much protection is adequate. However, the standard lacks specific definitions and guidance on how roles and responsibilities are established for managing cybersecurity risks across organizations both within the ministries and between the ministries and the OCIO.
- The selected ministries had organizational charts, job descriptions, service agreements and contracts that include information security roles and responsibilities, but they did not specifically refer to cybersecurity as one of the key responsibilities. Most of the organizations within these ministries did not maintain responsibility charts specific to cybersecurity.

RECOMMENDATION 1: We recommend that the Office of the Chief Information Officer, ministries and, when applicable, third-party providers work together to identify, establish and document cybersecurity roles and responsibilities for employees and for third-party stakeholders, including where those persons have a role in managing IT assets.

Maintaining inventories of IT assets

Having well-maintained IT asset inventories will help ministries identify where their assets are and their risk exposure in order to establish an appropriate strategy for protection from cybersecurity threats. We examined whether the selected ministries and related organizations

had maintained an inventory of the physical devices, systems, software platforms and applications they are responsible for. We also examined whether they had maintained an inventory of information systems used in business operations and hosted or owned by third parties. (See [Appendix B](#), criteria 1, 2 and 4)

We looked to see if the selected ministries and related organizations had:

- established policies and standard for identifying and inventorying IT assets to mitigate cybersecurity risk
- identified and inventoried IT assets
- based IT asset inventories on the assets' risk and the ministry's risk tolerance (e.g., systems that process, store or access sensitive information and/or are critical to business objectives)
- captured key and relevant information in the inventory records (e.g., asset name, type, version, owner, vendor/third-party provider and the staff responsible for maintaining and reviewing the inventory)
- implemented processes and tools to ensure that IT asset inventories were accurate, complete and current

For the five ministries and three related organizations we assessed, as noted in [Exhibit 2](#), we found that:

- other than OCIO-ES and the Ministry of Education, the organizations had not maintained an inventory of the physical devices and systems they were responsible for or the information systems used in business operations and hosted or owned by third parties
- other than the Ministry of Education, the organizations had not maintained an inventory of the software platforms and applications they were responsible for

Guidance for establishing reliable IT inventory records for cybersecurity purposes was lacking

Chapter 8 of the *Corporate Policy and Procedure Manual* requires each B.C. government organization to maintain and safeguard government assets coming under its custody or control. In addition, Chapter 12 states that corporate management of information and IT is the responsibility of the government chief information officer (GCIO).

The OCIO's Information Security Standard also has a chapter focused on IT asset management. The standard requires that:

- information owners identify assets under their control
- information owners and information custodians document, maintain and verify asset

inventories on a regular basis, depending on the criticality and value of the assets, and validate the measures taken to protect the assets as part of a risk management strategy

We reviewed these government policies and standards, designed to ensure that ministries identify the IT assets that need protecting, who should protect them and how they should be protected. We found that these documents lacked clear guidance on the establishment of reliable and robust inventory records for cybersecurity. For instance, they lack guidance on:

- what tool and methods to use for identifying and tracking IT assets
- what information is essential for inventorying IT assets
- how to prioritize IT assets in accordance with the ministries' and related organizations' cybersecurity risks

RECOMMENDATION 2: We recommend that the Office of the Chief Information Officer and the ministries collaborate to review and update core government policies and standards and ministry-specific guidelines in accordance with good cybersecurity practices regarding IT asset inventories.

Ministries did not use a consistent approach to identifying and inventorying IT assets

We examined IT asset inventory records to see if ministries used consistent tools and methodology to identify and track their IT assets. The use of consistent tools and methodology helps ensure completeness and accuracy in identifying and tracking IT assets for cybersecurity purposes across government. We found the following:

- All selected ministries and related organizations recognized the OCIO's asset registry and systems repository as the corporate standard for tracking applications.
- All selected ministries and related organizations used various tools to record IT assets—for example, Excel spreadsheets, Word documents, reports from different device management systems, and off-the-shelf applications. However, some of these tools were designed mainly for financial management purposes and not for identifying and tracking IT assets for cybersecurity purposes.
- The Ministry of Education used two different applications to track its physical devices and business applications. The natural resource ministries used different applications depending on the type of devices and business applications in use.

Furthermore, we noted that OCIO-ES used reports from a variety of reporting tools to capture information about physical devices. Some of these tools, provided by external service vendors, captured information such as asset name, serial number, type, version, location and so on, but each produced a report in a different format or with a different level of detail.

Inconsistent tools and methodologies adopted by the selected ministries make it difficult to ensure the completeness and accuracy of the inventory of IT assets.

RECOMMENDATION 3: We recommend that the Office of the Chief Information Officer and the ministries collaborate to adopt a consistent approach for identifying and tracking their IT assets to ensure the completeness and accuracy of inventories of IT assets.

Not all IT assets were captured, and inventories were missing key information

We examined the ministries' inventories of physical devices and systems, software platforms and applications, and information systems hosted or owned by third parties to determine whether they were complete and accurate. We expected that the inventories would:

- include IT assets that are used to collect, process, store and transmit information, and those that connect to their network and devices
- capture information essential for managing IT assets for the purpose of building a strong cybersecurity program for protection from internal and external threats

We found that the inventories of IT assets were incomplete and inaccurate. For example:

- The inventories did not include devices that have IP addresses and that can expose the ministries to security threats, such as VoIP (voice-over-internet protocol) phones, smart TVs, projectors, external/portable storage devices and internet of things devices (see glossary for definitions of these terms).
- The OCIO's asset registry and systems repository did not include all software platforms and applications. Lead OCIO IM/IT staff indicated that they had been working with the ministries to complete the asset registry and critical systems repository.
- Only the Ministry of Education, Government Communications and Public Engagement and the Financial Institutions Commission (FICOM), which was under the Ministry of Finance (FICOM became a Crown entity as of November 1, 2019, and is now called the BC

Financial Services Authority), had identified and tracked information systems used in their business operations and hosted or owned by third parties.

- Documentation of Ministry of Citizens' Services, Ministry of Finance, Ministry of Health, natural resource ministries, BC Public Service Agency and Government Communications and Public Engagement inventories were missing key information, such as asset name, version, owners (business or systems), third-party provider, location, and staff responsible for maintaining and reviewing inventories.

We also found that there was no evidence that the inventories of IT assets were based on the assets' risk and the ministries' risk appetite.

RECOMMENDATION 4: We recommend that the Office of the Chief Information Officer and the ministries collaborate to ensure that inventories are complete and accurate, based on the assets' risk and the ministries' risk appetite.

Ministries did not have a formal process, appropriate documentation or tool to ensure that IT asset inventories were complete

We assessed whether ministries performed periodic reviews to ensure that the inventories were complete, accurate and current. We expected to see formal procedures—review frequency, original data sources to compare with, sign-off after review, and delegation of the knowledgeable staff performing reviews—and the evidence that these procedures are carried out.

We found that none of the ministries and related organizations performed periodic reviews to verify the IT asset inventories. They indicated that they conducted periodic reviews; however, they did not have formal procedures for reviews and could not provide documentation to demonstrate that periodic and appropriate reviews were carried out.

An effective way to help organizations ensure that inventories of IT assets remain accurate, complete and current is to adopt an automated tool to detect and/or store inventories of all physical devices and systems (authorized and unauthorized, old and new). We found that the selected ministries did not have a process or system to auto-detect:

- authorized devices directly acquired from third parties and unauthorized devices connected to the network and other devices
- authorized and unauthorized applications downloaded by staff

- authorized and unauthorized information systems used in business operations that are hosted or owned by third parties

The use of an automated tool will help organizations remove or update, on a timely basis, any devices and applications that can make them susceptible to cyberattacks.

RECOMMENDATION 5: We recommend that the Office of the Chief Information Officer and the ministries collaborate to establish formal periodic reviews and/or adopt an automated tool for ensuring that records of IT assets are kept accurate, complete and current.

Maintaining maps of organizational communication and data flows

Maps of organizational communication and data flow can assist organizations in identifying their key data and their vulnerabilities to cybersecurity threats. These maps consist of network and data flow diagrams showing the flow of information between key processing areas and systems.

Flow control restrictions include keeping information from being transmitted unencrypted (in clear text) over the internet and blocking outside traffic that claims to be from within the organization. Therefore, it is important that these maps are kept current and contain key information, such as information flow within the system and between interconnected systems; devices and applications that are public-facing (internet accessible); and location of firewalls/routers to block unauthorized access.

Organizational communication and data flow maps were missing key information and were not kept accurate, complete or current

We examined whether the selected ministries had maintained maps of organizational communications and data flows (see [Appendix B](#), criterion 3). We looked to see if:

- key data flow and logical network maps had been completed
- diagrams captured key and relevant components (e.g., data, applications, hardware, devices, partner/third-party systems)
- processes had been implemented to ensure that maps are accurate, complete and current

We found that OCIO-ES had key core government network maps, and the ministries had their own maps in the form of network, infrastructure, server architecture and/or process maps. Only four of eight ministries had high-level data flow maps. Those maps were inconsistent and missing key information. For example, some were missing key components, such as flow control points, access points, routers, switches, firewalls, location code, date created and modified, revision numbers and staff responsible for maintaining the maps.

Furthermore, none of the ministries and related organizations had formal procedures for reviews or could demonstrate that periodic and appropriate reviews were performed to ensure that these maps were accurate, complete and current. Also, roles and responsibilities for maintaining maps of organizational communication and data flows across organizations both within the selected ministries and between the ministries and OCIO-ES were unclear.

RECOMMENDATION 6: We recommend that the Office of the Chief Information Officer and the ministries collaborate to develop specific guidelines and procedures for ensuring that maps of key organizational communication and data flows include key information and are kept accurate, complete and current.

Prioritizing IT assets based on classification, criticality and business value

Not all IT assets are equally important to an organization in achieving its business objectives. Therefore, prioritizing IT assets based on classification, criticality and business value can help an organization align and prioritize its cybersecurity activities with its business requirements, risk tolerances and resources.

With an understanding of risk tolerance, organizations can prioritize cybersecurity activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent.

IT asset inventories did not include classification, criticality and business value information

We examined whether the selected ministries had prioritized IT assets they are responsible for based on classification, criticality and business value (see [Appendix B](#), criterion 5). We looked to see if:

- the ministries had a current data classification program

- the data classification program provided a framework for classifying and prioritizing IT assets (hardware and other devices, systems software, applications, data) based on criticality and business value
- inventory documentation (physical devices and systems, software platforms and applications, and systems hosted by third parties) included asset classification, criticality and business value information

We found that the government had developed standards and guidelines for information security classification and critical systems, which ministries are expected to comply with. These standards and guidelines provide a framework for classifying and prioritizing IT assets based on criticality and business value. The OCIO also established a central asset registry for ministries to use for updating their inventory records of IT assets. The registry includes information security classification, criticality and business value information for ministry business applications. However, as mentioned above, the asset registry and systems repository did not include all software platforms and applications.

We also found that, besides the central asset registry, very few of the IT asset inventory documents contained information security classification, criticality or business value information. We were informed that ministries and related organizations prioritized their IT assets in preparing their business continuity plans, privacy impact assessments, and security threat and risk assessment plans. However, there was no clear linkage between those assessments and the prioritization as recorded in the central asset registry and other IT asset inventory documents.

RECOMMENDATION 7: We recommend that the Office of the Chief Information Officer and ministries collaborate to ensure that IT asset inventory records meet the expectations established in government standards and guidelines for classification, criticality and business value information based on risk assessments.

AUDIT QUALITY ASSURANCE

We conducted this audit under the authority of section 11(8) of the *Auditor General Act*. 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*. These standards require that we comply with ethical requirements and conduct the audit to independently express a conclusion on whether or not the subject matter complies in all significant respects to the applicable criteria.

The office applies the CPA Canadian Standard on Quality Control 1 (CSQC), 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 this respect, we have complied with the independence and other requirements of the code of ethics applicable to the practice of public accounting issued by the Chartered Professional Accountants of BC that are founded on the principles of integrity, objectivity and professional competence, as well as due care, confidentiality and professional behaviour.

GLOSSARY

anti-malware: Anti-malware solutions can range from basic to comprehensive end-point protection measures. These solutions should be able to detect and protect from various kinds of threat agents, such as viruses, worms, Trojans, spyware, adware, keyloggers and other variants of malware. (Source: ISACA)

application: A computer program or set of programs that performs the processing of records for a specific function. Contrasts with systems programs, such as an operating system or network control program, and with utility programs, such as copy or sort. (Source: ISACA)

cybersecurity: The protection of information assets by addressing threats to information processed, stored and transported by internet-worked information systems. It consists of technologies, processes and controls designed to protect systems, networks, computer programs, devices and data from cyberattacks. Effective cybersecurity reduces the risk of cyberattack and protects against the unauthorized exploitation of systems, networks and technologies. (Sources: ISACA and IT Governance UK)

device: A generic term for a computer subsystem, such as a printer, serial port or disk drive. A device frequently requires its own controlling software, called a device driver. Our audit also covered mobile devices, which are small handheld computing devices, typically having a display screen with touch input and/or a miniature keyboard and weighing less than two pounds. (Source: ISACA)

encryption: The process of taking an unencrypted message (plaintext), applying a mathematical function to it (encryption algorithm with a key) and producing an encrypted message (ciphertext). (Source: ISACA)

hardware: The physical components of a computer system. (Source: ISACA)

information systems: The combination of strategic, managerial and operational activities involved in gathering, processing, storing, distributing and using information and its related technologies. Information systems are distinct from information technology (IT) in that an information system has an IT component that interacts with the process components. (Source: ISACA)

information systems hosted or owned by third parties: External information systems, such as personally owned information systems/devices; privately owned computing and communication devices resident in commercial or public facilities; information systems owned or controlled by non-governmental organizations; and government information systems not owned by, operated by or under direct supervision and authority of organizations. Also includes accessing cloud services from organizational information systems for processing, storage or transmission of organizational information. (Source: NIST Special Publication 800-53 Revision 4, AC-20 Use of External Information Systems)

internet of things: The internet of things is the network of physical objects or “things” embedded with electronics, software, sensors and network connectivity, which enables these objects to collect and exchange data. The essence of the internet of things resides in the source of the data, which is the sensors. Those devices generate data about activities, events and influencing factors that provide visibility to performance and support decision processes across a variety of industries and consumer channels (e.g., pacemakers, smart TV, August smart lock, smart light bulbs). (Source: International Institute for Analytics)

logon: The act of connecting to the computer, which typically requires entry of a user ID and password into a computer terminal. (Source: ISACA)

malware: Short for malicious software. It is designed to infiltrate, damage or obtain information from a computer system without the owner's consent. Malware is commonly taken to include computer viruses, worms, Trojan horses, spyware and adware. Spyware is generally used for marketing purposes and, as such, is not malicious, although it is generally unwanted. Spyware can, however, be used to gather information for identity theft or other clearly illicit purposes. (Source: ISACA)

maps of organizational communication and data flows: For the purpose of this audit, these include diagrams that regulate where information is allowed to travel within an information system and between interconnected information systems. These are based on organization-defined information flow control policies. (Source: NIST Special Publication 800-53 Revision 4, AC-4 Information Flow Enforcement)

physical devices and systems: For the purpose of this audit, these include but are not limited to desktops, laptops, printers, scanners, multifunction devices, smart TVs, servers, network devices (e.g., firewalls, routers, switches), mobile devices (e.g., tablets, cell phones), IoT devices, personal storage devices and the firmware that runs these devices.

ransomware: Malware that restricts access to the compromised systems until a ransom demand is satisfied. (Source: ISACA)

software: Programs and supporting documentation that enable and facilitate use of the computer. Software controls the operation of the hardware and the processing of data. (Source: ISACA)

software platforms: For the purpose of this audit, software platforms are the operating system (OS), including web browser, application programming interfaces and other underlying software, in which applications are executed. Examples of OS are Microsoft Windows, MacOS, Unix, Linux, Mainframe, OpenVMS, Android and iOS. (Source: Wikipedia and others)

user credentials: In computer security, user credentials are typically some form of “username” and a matching “password,” and these credentials themselves are sometimes referred to as a login, a logon, a sign-in or a sign-on. In practice, modern secure systems often require a second factor, such as an email or SMS confirmation for extra security. (Source: Wikipedia)

VoIP (voice-over-internet protocol): Also called IP telephony, internet telephony and broadband phone; a technology that makes it possible to have a voice conversation over the internet or over any dedicated Internet Protocol (IP) network instead of over dedicated voice transmission lines. The terms internet telephony, broadband telephony and broadband phone service specifically refer to the provisioning of communications services (voice, fax, SMS, voice-messaging) over the public internet, rather than via the public switched telephone network, also known as the plain old telephone service. (Source: ISACA and others)

virtual private network (VPN): A secure private network that uses the public telecommunications infrastructure to transmit data. In contrast to a much more expensive system of owned or leased lines that can only be used by one company, VPNs are used by enterprises for both extranets and wide areas of intranets. Using encryption and authentication, a VPN encrypts all data that pass between two Internet points, maintaining privacy and security. (Source: ISACA)

web applications: Web applications differ from the traditional client-installed applications.

Web applications:

- are client-server applications that leverage a browser such as Microsoft Internet Explorer, Google Chrome, Apple Safari or the open source Firefox on the client side of the application
- are generally platform-independent—they will run on Windows, LINUX, Mac OS and even on mobile device platforms such as iOS and Android
- generally require less computational power than their client-based predecessors
- can be seamlessly integrated with a nearly limitless array of online resources and services (Source: ISACA)

APPENDIX A: NIST CYBERSECURITY FRAMEWORK CORE FUNCTIONS AND CATEGORIES

Functions organize basic cybersecurity activities at their highest level. Categories are the subdivisions of a function into groups of cybersecurity outcomes closely tied to program needs and particular activities.

1. **IDENTIFY**—Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
2. **PROTECT**—Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
3. **DETECT**—Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
4. **RESPOND**—Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
5. **RECOVER**—Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Function	Category
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes and Procedures
	Maintenance
Detect	Protective Technology
	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
	Response Planning
Respond	Communications
	Analysis
	Mitigation
	Improvements
	Recovery Planning
Recover	Improvements
	Communications

APPENDIX B: CRITERIA AND BASES OF ASSESSMENT VALIDATION

Criteria and bases of assessment validation

1. Ministry has maintained an inventory of physical devices and systems for which it is responsible.
 - 1.1 Has the ministry completed an inventory of physical devices and systems under its responsibility?
 - 1.2 Is the scope of the inventory based on the ministry's risk appetite (e.g., systems that contain sensitive information, allow access to the network, or are critical to business objectives)?
 - 1.3 Did the inventory documentation capture key/relevant information (e.g., asset name and number, type, version, location, owner, vendor, and the staff responsible for maintaining and reviewing the inventory)?
 - 1.4 Has the ministry ensured that the inventory is accurate, complete, and up to date?
For example:
 - a) use of automated software to detect and/or store inventory of all physical devices and systems (authorized and unauthorized, old, and new)
 - b) periodic inventory review
2. Ministry has maintained an inventory of software platforms and applications for which it is responsible.
 - 2.1 Has the ministry completed an inventory of software platforms and applications under its responsibility?
 - 2.2 Is the scope of the inventory based on the ministry's risk appetite (e.g., software that processes, stores, or accesses sensitive information or is critical to business objectives)?
 - 2.3 Did the inventory documentation capture key/relevant information (e.g., asset name, type, version, owner, vendor, and the staff responsible for maintaining and reviewing the inventory)?

2.4 Has the ministry ensured that the inventory is accurate, complete, and up to date?

For example:

- a) use of automated software to detect and/or store inventory of all software platforms and applications (authorized and unauthorized, old, and new)?
- b) periodic inventory review?

3. Ministry has maintained maps of organizational communication and data flows.

3.1 Has the ministry completed data flow diagrams, logical network diagrams, and/or other diagrams that show organizational communication and data flow?

3.2 Did the data flow diagrams, logical network diagrams, and other diagrams showing organizational communication and data flows capture key/relevant components (e.g., data, applications, hardware, devices, partners/third-parties' systems)?

3.3 Has the ministry ensured that the data flow diagrams, logical network diagrams, and/or other diagrams that show organizational communication and data flow are accurate, complete, and up to date (e.g., periodic review)?

4. Ministry has maintained an inventory of information systems used in business operations and hosted or owned by third parties.

4.1 Has the ministry (or third-party provider) completed an inventory of information systems used in business operations hosted or owned by third parties?

4.2 Is the scope of the inventory based on the ministry's risk appetite (e.g., systems that store, process, or access sensitive information or are critical to business objectives)?

4.3 Did the inventory documentation capture key/relevant information (e.g., systems name and number, type, version, hosting location, business purpose, user business group and primary contact, third-party provider or owner and the staff responsible for maintaining and reviewing the inventory)?

4.4 Has the ministry ensured that the inventory is accurate, complete, and up to date?

For example:

- a) use of automated software to detect and/or store inventory of all information systems hosted or owned by third parties (authorized and unauthorized, old, and new)
- b) periodic inventory review

5. Ministry has prioritized IT assets for which it is responsible based on classification, criticality, and business value.
 - 5.1 Does the ministry have a data classification program that is current?
 - 5.2 Does the data classification program provide a framework for classifying and prioritizing IT assets (hardware, software, devices, data) based on criticality and business value? (Note: Classification may also be identified in the risk assessment or business impact analysis.)
 - 5.3 Do the inventory documentations (physical devices and systems, software platforms and applications, and systems hosted by third parties) include asset classification, criticality, and business value information?
6. Ministry has defined and established cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners).
 - 6.1 Do the selected ministry's security policies, organization charts, job descriptions, agreements, RACI charts, service level agreements and contracts include cybersecurity roles and responsibilities?



OFFICE OF THE
Auditor General
of British Columbia

AUDIT TEAM

Cornell Dover,

Assistant Auditor General

David Lau,

Director, IT Audit

Joji Fortin,

Manager, IT Audit

Jenny Wang,

IT Auditor

Hiroko Griese,

Auditor

Kenneth Pomeroy,

Auditor

Justin Brajkovic,

Senior Audit Associate

Richard Davis,

Senior Audit Associate

LOCATION

623 Fort Street

Victoria, British Columbia

Canada V8W 1G1

OFFICE HOURS

Monday to Friday

8:30 am – 4:30 pm

Telephone: 250-419-6100

Toll-free through Enquiry BC: 1-800-663-7867

In Vancouver: 604-660-2421

FAX: 250-387-1230

EMAIL: bcauditor@bcauditor.com

WEBSITE: www.bcauditor.com

This report and others are available at our website, which also contains further information about the office.

REPRODUCING

Information presented here is the intellectual property of the Auditor General of British Columbia and is copyright protected in right of the Crown. We invite readers to reproduce any material, asking only that they credit our office with authorship when any information, results or recommendations are used.

