AUDIT AT A GLANCE

IT ASSET MANAGEMENT IN B.C. GOVERNMENT

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.

Objective

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.

Audit period: December 2017 to June 2019

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.

Government has accepted all 7 recommendations that we made to improve the management of IT assets.

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

OFFICE OF THE
Auditor General
of British Columbia

bcauditor.com

What we found (continued)

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

RECOMMENDATION 2

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

RECOMMENDATION 3

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)

RECOMMENDATION 4

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 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

RECOMMENDATION 6

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 7

After reading this report, you may wish to consider asking the following questions of government:

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?*