BRITISH COLUMBIA | Ministry of Citizens' Services

MISO 101 Guidebook

The basics of being a Ministry Information Security Officer in the Government of British Columbia

Information Security Branch

Ministry of Citizens' Services

Document Created October 2019

Updated February, 2020

"It is the responsibility of every employee to protect government information"

Gary Perkins, Chief Information Security Officer

Table of Contents

Introduction

Information is a valuable asset. The information that government collects, uses, maintains, stores, transmits and may eventually dispose of, is central to the work of every part of the government. All BC government employees are aware of their responsibility to protect that information to ensure public confidence. Although each employee is expected to protect the confidentially, integrity and availability of data, some employee roles carry more responsibility towards this objective. One of those roles is the Ministry Information Security Officer (MISO).

This guide is geared towards exploring in depth the key roles and responsibilities of the MISO. The guide contains information, tools and resources that will benefit MISOs in performing their role. This information will also benefit organizations and individuals beyond the role of the MISO who intend to improve the security of their enterprise.

What is a MISO

The Ministry Information Security Officer (MISO) is one of the primary contacts for information security issues and related concerns in their ministry.

The role of MISO comes with many key responsibilities that are important in protecting the information of their ministry and of the province. Below is a listing of the key responsibilities that are individually explored in depth in this document.

Specifically, the Ministry Information Security Officer is responsible for (Information security standard part 1.2.):

- Knowing the information security policy and standard requirements and communicating them within their ministries;
- Assisting business areas to understand and comply with information security policies and standards;
- Ensuring that procedures to support day-to-day security activities are per the Information Security Standard;

- Co-ordinating information security awareness and education activities and resources for their ministry;
- Providing up-to-date information on issues related to information security;
- Facilitating business areas with conducting Security Threat and Risk Assessments;
- Ensuring that each information system has a current System Security Plan;
- Providing advice on security requirements for information systems development and enhancements;
- Co-ordinating ministry information security initiatives with cross-government information security initiatives;
- Providing advice on emerging information security standards relating to ministry specific lines of business; and,
- Raising ministry security issues to the cross-government information security forums.

In addition to the list mentioned above, there are a few more responsibilities that fall onto the MISO to ensure that the information of the ministry and province is protected. Some of the extra responsibilities are addressed in the final section called "Other Tasks".

Key Responsibilities

Communicate the information security policy (ISP) and information security standards requirements within their ministries

One of the key responsibilities of the MISO is to have a high level of understanding of information security related policies and standards. By having a good understanding of the information security policies and information security standards, MISOs can communicate government's information security requirements to their ministries. This, in turn, will enable ministries to:

- Establish ministry policies and procedures necessary for the protection of information and technology assets for the Government of British Columbia.
- Determine how to apply the information security policies and information security standards in their business operations.
- Increase employees' awareness on their responsibilities to safeguard the information in their care.
- Improve government services by promoting consistent, appropriate management of government technology resources.

The three most important standards and policies for the MISO to understand are Information Security Policy (ISP), the Core Policy Procedures Manual (CPPM) (specifically CPPM Chapters 12 and 15) and the Information Security Standard (ISS). The ISP and CPPM provide the framework under which all ministries must operate in order to ensure the information security practices of the Government of British Columbia are reasonable, appropriate, and efficient. The ISS and other information security standards provide the framework for government organizations to protect government information and technology assets.

Below is a reference list of some of the most important BC Government standards and policies for a MISO to become familiar with:

- Information Security Policy (ISP)
- Core Policy Procedures Manual (CPPM), specifically:
    - CPPM Chapter 12
    - CPPM Chapter 15
    - CPPM Chapter 6 section 6.3.5
    - CPPM Chapter 8 (Asset Management)
    - CPPM Chapter 16 (Business Continuity Management)
    - CPPM Chapter 20 (Loss Management)
- Information Security Standard (ISS)

Other helpful resources to accompany the ISS, ISP and CPPM are:

- Appropriate Use Policy - establishes the policy requirements that all government employees and contractors must follow when accessing and managing government information and using information technology (IT) resources.
- Privacy Management & Accountability Policy (PMAP) - ensure ministries meet all of their legislative obligations while fostering a culture of privacy within government.
- Information Management Act (IMA) - the Government of British Columbia's legislative framework for modern, digital information practices.
- Information Incident Management Policy (IIMP) - Details the specific responsibilities of ministry employees, supervisors, service providers and the Ministry Chief Information Officer in the event that an information incident occurs.

For questions on policy or documentation please contact Information Security Advisory Services: infosecadvisoryservices@gov.bc.ca

Assist business areas to understand and comply with information security policies and information security standards

The ministries in the Government of British Columbia have many different business operations; some of which are unique.

The role of the MISO is to assist business areas when they are making decisions that may impact the security of information. The MISO will need to advise the business areas on the ISP and the applicable information security standards to ensure they remain in compliance with government information security requirements.

The IM/IT Standards Frequently Asked Questions is a good resource to assist business areas if there are questions in regards to standards and policies.

If business areas determine that their desired operations will not comply with a standard or policy, then they can request an exemption (which is a temporary measure) to the standard or policy. MISOs may need to assist, advise and occasionally approve exemption requests from business areas especially if they are impacting government information assets. MISOs should ensure that business areas review the exemption FAQs first. Once they have reviewed the FAQs, they can request an exemption.

If MISOs or business areas have further questions they can email:

- Infosecadvisoryservices@gov.bc.ca for questions on Information Security Policy
- EDS@gov.bc.ca for questions on IM/IT Standards
- IT.Policy@gov.bc.ca for questions on Chapter 12 of Core Policy

Ensure that ministry policies and standards support information security in day-to-day activities

Each ministry in the Government of British Columbia is responsible for a specific area of public policy, government function or service delivery. Due to the uniqueness of ministries there is also a uniqueness in day-to-day security activities. All day-to-day security activities within a ministry should have ministry-specific processes or standards supporting them. See Ministry IM/IT Policies and Standards page for more information.

The MISO role is to ensure that the processes and procedures to support day-to-day security activities are documented in compliance with the ISS as well as ministry specific standards. If a MISO or business areas are unsure of current ministry-specific standards, they can review them on their ministry websites.

If your ministry is creating its own specific standard, it should refer to the ISS for guidance. It can also seek peer review on the standard by contacting Advisory Services at infosecadvisoryservices@gov.bc.ca.

If your ministry has a policy group, you can contact them for assistance with policy development or documentation. Use https://dir.gov.bc.ca/ or check your ministry intranet page to look up the contact information for your ministry’s policy group.

Co-ordinate information security awareness and education

Information security awareness and education is an important part of the MISO role in protecting government assets and citizen information. It is through education that a MISO can help ministry employees to understand that they are all responsible for protecting government information.

Many security incidents within organizations are due to user error, which can come in the form of users clicking on a malicious link, giving away confidential information, leaving devices unattended etc. Security awareness can keep security in mind, which promotes a culture of security within an organization and thus, can decrease information security incidents.

A MISO can improve ministry employees' security awareness with ongoing outreach. The most important step for this outreach is to create a security awareness plan for the year. The security awareness plan provides a MISO a planned approach to security awareness that ensures constant engagement with ministry employees.

The awareness plan should outline all the methods, trainings, and activities that promote a security culture (e.g. social engineering exercises, security courses, etc.). This plan should typically span a year, be reviewed annually and have executive signoff.

Some items that a MISO can consider in their awareness plan;

- When to put up posters
- When to host presentations
- When to distribute specific awareness handouts
- When to distribute quizzes
- What event to host for security awareness month
- Who to bring in as a guest speaker
- Identifying key stakeholders
- Assigning security ambassadors to assist with the program

Below are some resources that will help with awareness;

- **Awareness Repository**: This is where you can find the security awareness material produced by the OCIO (Guidebooks, posters, pdfs, policies, etc.).
- **Security News Digest**: This is a weekly email with a collection of the latest information security news articles.
- **Thought Papers**: A collection of papers on emerging trends and technologies.
- **Quizzes:** A collection of quizzes is an opportunity to test yourself on other information security topics.
- **Information Security Page:** This is the main landing page for information security.

Some popular security events that you might want to bring to the attention of your ministry employees;

- **Security Day**: This is a twice a year event that brings together security experts across the province to discuss relevant security topics. The event is also webcasted.
- **Privacy and Security Conference**: The Privacy and Security Conference has been one of the most popular conferences in Canada on the issues of privacy and security globally.
- **Cyber Awareness Month**: Each October, the federal government and a coalition of security organizations and agencies launch a campaign to provide information, tips and tools to inform the public of the importance of cyber security.
- **Pink Shirt Day**: Each February, people are encouraged to practice kindness and wear pink to symbolize that you do not tolerate bullying. Anti-cyber bullying now plays a major part in this campaign.
- **World Password Day:** Occurs every year on the first Thursday of May. This day reminds people about the importance of protecting themselves through strong passwords.

Provide up-to-date information on issues related to information security

Information Security is a fast-moving topic and involves threat actors who will try to use every advantage they can to compromise systems and data. Within the government, we need to constantly share the specific threats and incidents that we see with each other so that we can all be prepared and adequately defend ourselves.

Staying informed about what others are seeing is key. Here are a few resources available to MISOs to keep them current on security trends:

- **Vulnerabilities Reports:** Vulnerabilities that are identified in the open domain. These reports will help you to identify whether the vulnerabilities are relevant to your ministry or not and what others to be notified of. There is currently a SharePoint with vulnerability notifications.
- **Information Security Advisory Committee (ISAC) Meetings:** This is a monthly meeting with all the MISOs in government. It provides an opportunity to network and learn from your fellow peers as well as to inform them of what you are seeing in your ministry.
- **ISACA Victoria Chapter**: ISACA (previously the Information Systems Audit and Control Association) is a world-wide association of information security governance professionals. Being a member of ISACA you will be able to attend educational lunch and learns on timely security topics as well as network with security professionals and discuss current trends.
- **Security Day:** A twice-a-year event hosted at the OCIO that brings together security professionals and organizations across BC to discuss relevant security topics.
- **Security News Digest:** A listing of current security news articles sent out by the OCIO every Tuesday.
- **Information Sharing Conference call:** This is a monthly OCIO conference call where information relating to events, incidents, vulnerabilities, and mitigation strategies will be presented.
- **Awareness Program:** An email update containing key awareness materials such as posters, quizzes, educational handouts, videos and upcoming events.

For more information on any of these services please email: OCIOSecurity@gov.bc.ca

Facilitate Security Threat and Risk Assessments (STRAs) with business areas

Security Threat and Risk Assessments (STRAs) are a type of assessment used by the Government of British Columbia to assess digital risks. This is a key enabler for a responsible digital government. STRAs are a snap-shot in time that effectively raises the awareness on information system security risks in an organization to the level at which risk-based decisions are made. Management is responsible and accountable for information assets that are directly or indirectly under their control. STRAs are key to empowering them to make informed risk-based decisions about their information assets. A STRA also documents risk ratings and planned treatments for the identified risks.

One of the MISO responsibilities is to facilitate business areas within the ministry with STRAs. A STRA process has been published to assist with this; if your ministry has it’s own STRA process you may use this as well. This process supports MISOs and business areas with the collection of the necessary information to successfully complete a Statement of Acceptable Risk (SOAR).

Resources for a STRA:

- Assessment Process - The corporate process for conducting Security Threat and Risk Assessments.
- Outputs – What are the outputs of a STRA.
- Tools and Templates – STRA template, SOAR template and guidelines.

If you have any questions on completing STRAs, please email: InfoSecAdvisoryServices@gov.bc.ca

Ensure that each information system has a current System Security Plan (SSP)

As a MISO, one of your tasks is to ensure that each information system has a System Security Plan (SSP) that is current and up-to-date. The SSP is a living document and will need to be reviewed and updated at minimum annually or whenever a change/upgrade is made to the information system. An indirect change/upgrade to the information system (e.g. change of ownership, changes to business process(s) supporting the information system, roles & responsibilities related to the information system, the network environment in which it operates, other information systems connecting to it, information being processed, stored or transmitted through it, etc.) can also be a trigger to review/update the SSP for the information system.

A System Security Plan records information about, and decisions regarding, the development and deployment of information systems (ref: Security Standard for Application and Web Development and Deployment). The SSP consists of the following:

- A Privacy Impact Assessment;
- A summary of risks identified in the Security Threat and Risk Assessment i.e. STRA findings and recommended changes/remediation (ref: Communication Security Standard);
- Procedures and standards used to mitigate the STRA risks and to protect the information system and network;
- All security controls specific to the development and deployment of the information system;
- Specific procedures and standards used to mitigate risks and protect the information system and the network;
- Documented acceptance tests and approval of the acceptance testing results
- Results of the system certification (and accreditation if applicable) on the information system (ref: System Acquisition, Development and Maintenance Security Standard);
- Roles and responsibilities for the information system security and network security management;
- Roles and responsibilities of personnel responsible for managing the information and associated systems;

- Monitoring and operating procedures for the information system and network (including monitoring frequency, review and remediation processes);
- Documented security vulnerabilities that were identified to impact software applications used by the information system;
- A log of all patch management activities for the information system;
- A log of all approved changes and associated risks (and mitigations) for those changes;
- Communication procedures for security relevant events and incidents;
- Up-to-date Business Continuity and Disaster Recovery Plans for the information system, and
- Documented approvals for deploying the information system and all proposed changes to the system.

Other standards which will aid you in building your System Security Plan are:

- Critical Systems Standard
- Database Security Standard

For questions on developing a *System Security Plan (SSP)*; please email InfoSecAdvisoryServices@gov.bc.ca

Provide advice on security requirements in information systems development or enhancements

If someone within your ministry wishes to make changes or enhancement to an information system, you can assist them with understanding the ISP section 6 Information System Procurement, Development and Maintenance.

This section defines the requirements to ensure strong security controls are included in business and contract requirements for building and operating secure information systems, including commercial off the shelf and custom-built software.

Ministries must:

(a) Develop, implement and manage the processes and procedures necessary to ensure that information security risks and privacy requirements are considered throughout the systems development lifecycle;

(b) Ensure enough resources and funding are allocated to complete the necessary information security tasks;

(c) Ensure that system development or acquisition activities are aligned with government information security requirements and standards;

(d) Apply vulnerability scanning, security testing, and system acceptance processes commensurate to the value and sensitivity of the information system.

The Office of the Chief Information Officer provides corporate direction and oversight for developing and implementing security standards to procure, develop and maintain information systems. Additional resources: CPPM Chapter 6: Procurement, Information Security Standard (at: IM/IT Standards), and Security Standard for Application and Web Development and Deployment.

Co-ordinate ministry information security initiatives with cross-government information security initiatives

Cybersecurity is a top concern for all ministries within the Government of British Columbia. Therefore, one of the MISO responsibilities is to ensure that ministry information security initiatives are co-ordinated with cross-government information security initiatives to effectively address cybersecurity.

This responsibility involves communicating on the current security initiatives or future security initiatives your ministry is planning. By communicating on your current or future initiatives, it will help you to understand what work has already been accomplished as well as areas to co-ordinate efforts. This will also enable you to leverage off each other's efforts and reduce duplication of work, for example in STRAs. By sharing STRAs and SOARs, much of the effort involved in conducting STRAs need not be duplicated.

To assist you with collaborating with your fellow MISOs, the ISB has established the following avenues to come together and meet:

- **ISAC:** This is a monthly meeting with all the MISOs in the government. This is your opportunity to network and learn from your fellow MISOs as well as to inform them of what you are seeing in your ministry.
  Please contact Advisory Services: infosecadvisoryservices@gov.bc.ca to sign up for this meeting.
- **Information Sharing Conference call:** This is an OCIO conference call where information relating to events, incidents, vulnerabilities, and mitigation strategies will be presented.
  Please email: OCIOSecurity@gov.bc.ca for more information.
- **Networking functions:** There are many different networking functions and opportunities to connect with to other security professionals such as Security Day, Privacy and Security Conference, ISAC, meet up groups and OCIO Connect.
  Please email: OCIOSecurity@gov.bc.ca for more information.
- Ministry Information Security Officer (MISO) Internal page – For a list of government MISOs.

If you require assistance in implementing cross-government information security initiatives or are unsure of your role in a specific initiative, please email: InfoSecAdvisoryServices@gov.bc.ca

Provide advice on emerging information security standards relating to ministry specific lines of business

Information Management / Information Technology (IM/IT) standards are intended to improve government services by promoting consistent, appropriate management of government technology resources. They support core government policy, particularly chapter 12 on information management and information technology management.

As the security threat environment is constantly changing, so must information security standards. MISOs need to stay up to date on emerging new information security standards as well as on updates to the existing standards so that they can inform their ministry lines of business of the possible security impacts resulting from these changes.

Review the IM/IT standards and attend monthly ISAC meetings to stay up to date with current information security standards.

Please email: EDS@gov.bc.ca if you have any questions.

Raise ministry security issues to the cross-government information security forum

In your role as the MISO, you are likely to come across ministry specific security issues. When those issues arise, you should work to bring them to the attention of the cross-government information security forum. Sharing these security issues will allow others to learn form your successes and failures while you learn from theirs and ensure there is no unnecessary duplication of work. It will also help you to accomplish your mandates as a MISO.

For resources to help you to connect please see the resources listed in the "Co-ordinate ministry information security initiatives with cross-government information security initiatives" section.

Other tasks

Investigate reported information security events to determine if further investigation is warranted

As a MISO, you are the key ministry contact for individuals within your ministry who have experienced or are experiencing information security events to seek advice about such events.

If you receive a call or email regarding a potential event, you should:

1) Confirm that the affected employee has reported the potential incident to their manager or supervisor and has followed the four steps outlined in the Privacy Breaches web page.
2) Ensure that the individual has disconnected from the network and that the affected device is left powered on to prevent any damage to potential forensic evidence.
3) Provide the individual with the Information Incident Checklist (or your ministry's checklist, if you have a ministry specific one).
4) If the information breach involved a loss of a physical information technology asset, e.g. mobile devices, flash drive, laptop, etc., report the loss to the Risk Management Branch via the General

Incident Loss Report (GILR) within 24 hours. For more information on loss reporting you can visit the CPPM Procedure Chapter L: Loss Reporting page.

5) Work with the investigators and others involved to determine the specifics of the incident, to resolve it and if necessary, notify the stakeholders.
6) Provide security advice to the individual on appropriate actions to limit impact of the information breach.
7) Review the incident with the investigators and other necessary stakeholders to define and implement remediation measures to reduce/prevent similar occurrences in the future.

An incident is a security event that compromises the integrity, confidentiality and availability of an information incident. A breach is an incident that results in the confirmed disclosure of data to an unauthorized party. Understanding what led to your client's incident can help you to determine areas for awareness education within your ministry and further ways to ensure that this same event does not repeat itself. To learn about the incident response process that the investigation team uses when analyzing an incident, please visit the Cyber Security Incident Response Page.

If you are unsure of specific responsibilities of ministry employees, supervisors, service providers and the Ministry Chief Information Officer in an incident, review the Information Incident Management Policy.

Please contact: Privacy.helpline@gov.bc.ca if you have questions or concerns about an information incident.

Address IT Security related audits

Internal audits improve the efficiency, effectiveness, economy and accountability of public sector programs. There are four types of internal audits that will occur in the Government of British Columbia. These can be viewed at Internal Audits for Government & Broader Public Sector page.

One of the reviews that may involve MISOs is the Information Technology Review. This type of review will address business, privacy and security risks and strengthen the government's overall information management process. If the audit deems that there are specific actions required to improve ministry security, you as the MISO may need to assist the ministry business areas to complete actions laid out.

Please contact Internal Audit & Advisory Services at IAACTION@gov.bc.ca for more information.

Perform Ministry Security Assessments Using Defensible Security Framework

Cyber security is an ever-evolving industry and the cyber landscape keeps changing. Security controls that were adequate a few years ago have become obsolete today. As such, a MISO should take proactive steps to regularly assess their organization in order to identify areas of improvement and ultimately determine their organization's security posture. Security assessments will also assist the organization understand where to invest resources to mitigate risks and prevent exploitation of vulnerabilities that may disrupt operations and cause reputational damage.

The Province of British Columbia has defined a list of critical security controls in the Defensible Security for Public Sector Organizations manual, to assist organizations in assessing their security posture. The Defensible security framework consists of 25 control areas deemed necessary for an organization to maintain an optimal cyber hygiene level and be compliant with BC government policies.

For more information on Defensible Security visit www.Gov.BC.CA/Defensible-Security or contact the OCIOSecurity@gov.bc.ca if you have any questions.

Assessing and Addressing Information Security Vulnerabilities

A vulnerability is a weakness which can be exploited by a cyber attack to gain unauthorized access to a system or perform unauthorized actions on a system. Vulnerability scans completed by the Information Security Branch will identify areas that are susceptible to cyber attack. If high or critical risk vulnerabilities are detected in a Ministry, the Vulnerability and Risk Management team will contact the Ministry MISO and inform them of the potential risk. Once a MISO receives notification of vulnerabilities in their ministry the MISO should:

- Report the system vulnerability to the system owner
- Have owner fix/patch the current vulnerability
- Follow up with the owner to ensure that the vulnerability was successfully fixed/patched

Understanding and staying up to date with recent vulnerabilities will assist information security professionals in protecting information from threat actors. Below are vulnerability resources that can help MISOs stay up to date on timely vulnerabilities.

Canadian vulnerability sites resources:

- Canadian Centre for Cyber Security (CCCS) https://cyber.gc.ca/en/alerts-advisories
- National Institute of Standards and Technology (NIST) Network Information Security & Technology News https://www.nist.org/
- (NIST) National Vulnerability Database https://nvd.nist.gov/general/nvd-dashboard
- Exploit Database https://www.exploit-db.com/
- Government of BC Vulnerability and Risk Management Page (Internal) - https://intranet.gov.bc.ca/thehub/ocio/ocio-enterprise-services/information-security-branch/vulnerability-and-risk-management

Vendor specific vulnerability resources:

- CISCO https://tools.cisco.com/security/center/publicationListing.x
- Microsoft Security Update Guide https://portal.msrc.microsoft.com/en-us/security-guidance
- Adobe Security Bulletins and Advisories https://helpx.adobe.com/ca/security.html
- Oracle Security Alerts https://www.oracle.com/security-alerts/

For any questions on dealing with vulnerabilities, please contact VulnerabilityandRiskManagement@gov.bc.ca

Questions or Concerns

If you have questions or concerns regarding the information contained in the MISO handbook or if you are wishing to add further links or resources, please contact InfoSecAdvisoryServices@gov.bc.ca.