BRITISH
COLUMBIA

Ministry of
Citizens' Services

OPERATIONS SECURITY STANDARD

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.0

Published: September 2019

Table of Contents

I Introduction, Scope, Background

This standard is designed to be read in conjunction with the Information Security Standard (version 2.0) as it is a sub-section or sub-standard of the Information Security Standard (version 2.0) (published here: IM/IT Standards).

II Glossary, Terms and definitions, List of commonly used references

To avoid repetition of content, please check the "Glossary", "Terms and definitions" and "List of commonly used references " sections of the Information Security Standard (version 2.0) (published here: IM/IT Standards) for the terms and definitions used in this standard.

1 Operations Security

This chapter establishes a framework to support the integration of information security in the services provided by government information processing facilities. Planning and management of the day-to-day activities is required to ensure the availability and capacity of the resources that provide information services. This framework identifies requirements to control and monitor operations for service delivery and to manage changes as the operations evolve. For critical systems additional requirements are defined in the Critical Systems Standard.

Controls for operations include documented processes, employee duties and formal methods to implement changes to facilities. This includes methods to protect information, create copies for back-ups and to manage the media where those copies are stored. Network protection requirements from threats such as viruses or unauthorized disclosure are also described.

1.1 Operational Procedures and Responsibilities

1.1.1 Operating procedures and responsibilities for information systems and information processing facilities must be authorized, documented, and maintained.
a) Operating procedures

Purpose: ***To ensure correct operations of information systems and information processing facilities.***

1.1.1 a) Operating procedures
Information Custodians must ensure that approved operating procedures and standards are:

- Documented;
- Consistent with government policies, standards and guidelines; and
- Reviewed and updated annually or when there are:
  - Alterations to building layouts,
  - Changes to equipment/systems located in the facility,
  - Changes in business services and the supporting information systems operations, and,
  - As part of any related security incident investigation.

Operations documentation must contain detailed instructions regarding:

- Information processing and handling;
- Last review and update;
- Classification of document;
- System re-start and recovery;
- Back-up and recovery, including on-site and off-site storage;
- Exceptions handling, including a log of exceptions;
- Output and media handling, including secure disposal or destruction;
- Audit and system log management;
- Change management including scheduled maintenance and interdependencies;
- Computer room management and safety;
- Information Incident Management Process;
- Disaster recovery;
- Business continuity; and,
- Operations, technical, emergency and business contacts.

Recommended Tests:

Note: 1.1.1 is reported on as part of the annual information security review.

- Demonstrate all operational procedures are documented and maintained to current operations.

1.1.2 Changes to information systems and information processing facilities must be controlled.
a) Planning changes
b) Change management process
c) Implementing change

Purpose: ***To ensure changes to information systems and facilities are applied correctly and do not compromise the security of information and information systems.***

1.1.2 a) Planning changes

Information Owners and Information Custodians must plan for changes to information systems and information processing facilities by assessing the impact of the proposed change on security by conducting a security review based on the size of the change.

1.1.2 b) Change management process

Information Owners and Information Custodians must plan, document and implement a change management process to control changes by:

- Identifying and recording significant changes;
- Assessing the potential impact, including the security impact, of the change by conducting a Security Threat and Risk Assessment;
- Developing an implementation strategy;
- Obtaining approval of changes from the manager(s) responsible for the information system;
- Planning and testing changes including documenting fallback procedures;
- Communicating change details to relevant employees;
- Identifying the impact on agreements with business partners and third parties including information sharing agreements, Memoranda of Understanding, licencing and provision of services;
- Evaluating that planned changes were performed as intended; and,
- Training technical and operations employees if required.

1.1.2 c) Implementing changes

Information Owners and Information Custodians must implement changes by:

- Notifying affected parties, including business partners and third parties;
- Completing re-certification and re-accreditation as required prior to implementation;
- Training employees if required;
- Documenting and reviewing the documentation throughout the testing and implementation phases;
- Recording all pertinent details regarding the changes; and,
- Checking after the change has been performed that only the intended changes took place.

Recommended Tests:

Note: 1.1.2 is reported on as part of the annual information security review.

- Demonstrate a change management approval process exists.
- Demonstrate that changes are planned through collaboration with affected parties.
- Demonstrate all procedural documents are updated as part of the change management process.
- Demonstrate that changes are implemented in accordance with an approved change request agreement.
- Demonstrate that a Security Threat and Risk Assessment and Privacy Impact Assessment are part of the change plan process.
- Demonstrate emergency change management capabilities exist to enable a quick and controlled response to resolve an incident(s).

1.1.3 Controls must be applied to limit opportunities for information leakage.
a) Preventing information leakage

Purpose: ***To protect information and information systems from unauthorized access, theft or misuse.***

1.1.3 a) Preventing information leakage

Information Owners and Information Custodians must implement processes to reduce the opportunity for information leakage in information systems by:

- Scanning for malicious code;
- Monitoring resource usage in information systems;
- Identifying and limiting the trusted connections in and out of the government network;
- Controlling third party network connections (e.g., only authorized traffic permitted);
- Using software that is considered to be of high integrity;
- Regular monitoring of information systems; and
- Reviewing usage and access logs for irregularities.

Guidelines:

Scanning outbound media and communications for hidden information should be considered. Canadian Common Criteria Scheme (CCCS) certification may be considered for evaluation of high integrity software.

Recommended Tests:

Note: 1.1.3 is not reported on as part of the annual information security review.

- Demonstrate process controls for mitigating data leakage.
- Demonstrate logs are regularly reviewed for data in transit.

1.1.4 The use of information system resources must be monitored, optimized and projections made of future capacity requirements.
a) Resource capacity management
b) Resource capacity planning

Purpose: ***To reduce the risk of system failures and unacceptable performance levels by monitoring and optimizing resources to meet current and future information system capacity requirements.***

1.1.4 a) Resource capacity management

Information Custodians are responsible for implementing capacity management processes by:

- Documenting capacity requirements and capacity planning processes;
- Identifying and managing storage requirements;
- Including capacity requirements in service agreements;
- Monitoring and optimizing information systems to detect impending capacity limits; and,
- Projecting future capacity requirements based on:
    - New business and information systems requirements,
    - Statistical or historical capacity requirement information, and,
    - Current and expected trends in information processing capabilities (e.g., introduction of more efficient hardware or software).

1.1.4 b) Resource capacity planning

Information Custodians must use trend information from the capacity management process to identify and remediate potential bottlenecks that present a threat to system security or services. Information Owners and Information Custodians must plan and budget for business and service capacity management.

Guidelines:

Resource capacity management processes should be automated where feasible.

Recommended Tests:

Note: 1.1.4 is reported on as part of the annual information security review.

- Demonstrate capacity management process is documented and reviewed regularly.
- Demonstrate capacity planning has been completed for critical systems for the projected life of the system (e.g., capital planning, business case).
- Demonstrate information project planning considers additional capacity demand.

1.1.5 Development and test information systems must be separated from operational information systems.
a) Separation requirements

Purpose: ***To reduce the risk of unauthorized or inadvertent changes to operational information systems.***

1.1.5 a) Separation requirements

Information Custodians must protect operational information systems by:

- Separating operational environments from test and development environments (e.g., using different computer rooms, servers, domains and partitions);
- Preventing the use of test and development identities and credentials for operational information systems;
- Storing source code (or equivalent) in a secure location away from the operational environment and restricting access to specified employees;
- Preventing access to compilers, editors and other tools from operational information systems;
- Using approved change management processes for promoting software from development/test to operational information systems;

- Prohibiting the use of operational data in development, test or training information systems; and,
- Prohibiting the use of personal or sensitive information in development, test or training information systems.

Separating duties between development, test and operational information systems will assist in achieving the separation of systems.

Recommended Tests:
Note: 1.1.5 is reported on as part of the annual information security review.

- Demonstrate architecture diagrams illustrate clear separation between development, test, production environments and operational systems.
- Demonstrate a Security Threat and Risk Assessment identified the separation and the required controls for development, test, and production environments.
- Demonstrate that a Privacy Impact Assessment has been completed for all systems with personal information.

1.2 Protection from malware

1.2.1 Security awareness, prevention and detection controls must be utilized to protect information systems against network and host-based threats.
a) Prevention and detection controls
b) User awareness

Purpose: ***To protect the integrity of information systems and software through requirements for the prevention and detection of network and host-based threats.***

1.2.1 a) Prevention and detection controls
Information Custodians must protect government information systems from network and host-based threats by undertaking such activities as:

- Installing, updating and consistently using software designed to scan for, detect and provide protection from network and host-based threats;
- Prohibiting the use of unauthorized software;
- Checking files, including electronic mail attachments and file downloads for malware before use;
- Maintaining business continuity plans to recover from security incidents;
- Regularly reviewing file and data content on critical systems to identify unapproved or unauthorized files and file changes; and
- Scanning back-up media prior to restoration so that malware is not introduced or re-introduced into an information system and network.

The Chief Information Security Officer must ensure processes are implemented to:

- Maintain a critical incident management plan to identify and respond to security incidents; and,
- Maintain a register of specific threat countermeasures (e.g., blocked websites, blocked electronic mail attachment file types, blocked network ports, additional monitoring, etc.) including a description, the rationale, the approval authority and the date applied.

1.2.1 b) User awareness

The Chief Information Security Officer is responsible for developing user awareness programs for threat countermeasures.

Ministry Information Security Officers are responsible for communicating technical advice and providing information and awareness activities regarding network and host-based threats.

Employees are required to complete the information protection courses provided by the Public Service Agency as part of their awareness training.

Recommended Tests:
Note: 1.2.1 is reported on as part of the annual information security review.

- Demonstrate that devices connecting to government networks have an up-to-date anti-malware solution in place or other similar security measures.
- Demonstrate that employees have been provided with awareness training related to the protection of information (e.g., malware, phishing, spam).

1.3 Backup

1.3.1 Information and information systems must be backed up and the recovery process tested regularly.
a) Defining requirements
b) Safeguarding backup facilities and media
c) Testing

Purpose: To enable the timely recovery of information and information systems.

1.3.1 a) Defining requirements
Information Owners and Information Custodians must define and document backup and recovery processes that reflect the security classification and availability requirements of information and information systems including:

- Confirming that the backup and recovery strategy complies with:
  - Business continuity plans,
  - Policy, standard, legislative, regulatory and other legal obligations, and,
  - Records management requirements, including the Administrative Records Classification System (ARCS) and Operational Records Classification System (ORCS), and,
- Documenting the backup and recovery processes including:
  - Types of information to be backed up,
  - Schedules for the backup of information and information systems,
  - Backup media management (e.g., retention period, pattern of backup cycles),
  - Methods for performing, validating and labelling backups, and,
  - Methods for validating recovery of the information and information system.

1.3.1 b) Safeguarding backup facilities and media
Information Custodians must conduct a Security Threat and Risk Assessment to identify safeguards for backup facilities and media that are commensurate with the value and sensitivity of the information and information systems. Safeguards include:

- Using encryption to protect the backed up information;

- Using digital signatures to protect the integrity of the information;
- Physical and environmental security;
- Access controls;
- Methods of transit to and from offsite locations (e.g., by authorized couriers, by encrypted electronic transfer);
- Storage of media adhering to manufacturer recommendations for storage conditions and maximum shelf-life; and,
- Remote storage of backup media at a sufficient distance to escape any damage from a disaster at the main site.

1.3.1 c) Testing
Information Custodians must regularly test backup and recovery processes.

Recommended Tests:
Note: 1.3.1 is reported on as part of the annual information security review.

- Demonstrate access controls on backup data.
- Demonstrate that backup media is properly secured commensurate with the information sensitivity (e.g., encryption of personal information).
- Demonstrate backups are stored at a sufficient distance from the main site.
- Demonstrate restoration procedures are documented.
- Demonstrate a successful backup restoration has been completed.

1.4 Logging and monitoring

1.4.1 Audit logs must be produced, retained and regularly reviewed.
a) Audit logging
b) Review of monitoring activities
c) Audit log retention
d) Response to alarms

Purpose: To ensure usage of information systems can be monitored and audited.

1.4.1 a) Audit logging
Information Owners and Information Custodians must ensure that audit logs are used to record user and system activities, exceptions, and information security and operational events including information about activity on networks, applications and systems. Information Owners and Information Custodians will determine the degree of detail to be logged based on the value and sensitivity of information assets, the criticality of the system and the resources required to review and analyze the audit logs.

Audit logs must include, when relevant, the following information:

- User identifier;
- Dates, times and details of key events (e.g., logon and logoff);
- Logon method, location, terminal identity (if possible), network address;
- Records of successful and unsuccessful system logon attempts;
- Records of successful and unsuccessful data access (including record and field access where applicable) and other resource access attempts;
- Changes to system configuration;

- Use of privileges;
- Use of system utilities and applications;
- Files accessed and type of access (e.g., view, read, modify, delete);
- For voice calls: source and destination telephone numbers, date, time, and length of call;
- Name and size of file attachments that are part of or are included in data transmissions (e.g., email, instant messaging, unified communications platforms, etc.);
- Network addresses (source and destination), ports (source and destination), protocols, and transferred network data traffic flow (packets and bytes);
- Alarms raised by the access control system; and,
- Activation and de-activation of protection systems (e.g., anti-virus, intrusion detection).

Audit logs may contain confidential data and access must be restricted to employees with need-to-know privileged access and be protected accordingly. Information Owners and Information Custodians must not have the ability to modify, erase or de-activate logs of their own activities.

If audit logs are not activated, this decision must be documented and include the name and position of the approver, date and a rationale for de-activating the log. Where required, the Privacy Impact Assessment and Security Threat and Risk Assessment must be updated to reflect this decision.

1.4.1 b) Review of monitoring activities
Information Custodians must set up and document processes for the review of audit logs based on the Information Owners assessment of the value and sensitivity of the information assets, the criticality of the system and the resources required for review.

Audit log reviews must:

- Prioritize reviews of high value and highly sensitive information assets;
- Be based on a documented Security Threat and Risk Assessment; and
- Utilize automated tools to identify exceptions (e.g., failed access attempts, unusual activity) and facilitate ongoing analysis and review.

Monitoring must be tested at least annually to ensure that desired events are detected. Analysis of monitoring activities can indicate:

- The efficacy of user awareness and training and indicate new training requirements;
- Vulnerabilities that could be, or that are being, exploited; or
- Increases or decreases in unauthorized access attempts or unauthorized use of privileges.

1.4.1 c) Audit log retention
Audit logs must be:

- Retained according to the approved records retention schedule for the system or information asset; and,
- Retained indefinitely if an investigation has commenced which may require evidence be obtained from the audit logs.

1.4.1 d) Response to alarms
Information Custodians must establish and document alarm response procedures in collaboration with Information Owners to ensure alarms are responded to immediately and consistently. Information Custodians should have documented authority to shut down all or part of a system or network when the

alarm indicates new unacceptable threats are present. When exercising this authority, Information Custodians must report the circumstances to the Information Owners as soon as possible.

Normally, the response to an alarm will include:

- Identification of the alarm event;
- Isolation of the event including affected assets;
- Identification and isolation or neutralization of the source;
- Corrective action;
- Forensic analysis of event;
- Action to prevent recurrence; and,
- Securing of audit logs as evidence.

Recommended Tests:
Note: 1.4.1 is reported on as part of the annual information security review.

- Demonstrate that information systems audit logs capture the required information.
- Demonstrate logs are retained and reviewed.
- Demonstrate alarms are properly monitored.

1.4.2 Information system logging facilities and log information must be protected against tampering and unauthorized access.
a) Protecting information system logging facilities
b) Protecting log information

Purpose: To preserve the integrity of information system logging facilities and log information.

1.4.2 a) Protecting information system logging facilities
Information Owners are responsible for ensuring periodic independent reviews or audits are conducted to confirm that Information Custodians have implemented appropriate controls.

Information Custodians must implement controls to protect logging facilities and log files from unauthorized modification, access or disposal. Controls must include physical security safeguards such as situating logging facilities within a secure zone with restricted access.

1.4.2 b) Protecting log information
Information Custodians must apply controls to protect log files from tampering or modification. Controls must include:

- Consideration of multi-factor authentication for access to sensitive records;
- Back-up of audit logs to off-site facilities;
- Automatic archiving of audit logs to remain within storage capacity;
- Scheduling the audit logs as part of the records management process; and,
- Digital signing for detecting alteration or corruption where available.

All employees must not have permission to erase logs or de-activate logging of their own activities.

Recommended Tests:
Note: 1.4.2 is reported on as part of the annual information security review.

- Demonstrate logging information is accurate and meets business needs.

- Demonstrate that the logs are restricted to authorized employees (e.g., access to the logs must be logged).
- Demonstrate that logs are read-only.

1.4.3	**Activities of privileged users must be logged, and the log must be subject to regular independent review.** **a) Activities logged** **b) Independent review**

Purpose: ***To protect government information from unauthorized access, modification or deletion.***

1.4.3 a) Activities logged

Privileged users typically have extensive system permissions not granted to most users. Information Owners and Information Custodians must ensure that the activities of privileged users are regularly reviewed, including logging:

- Event occurrence times;
- Event details, such as files accessed, modified or deleted, errors and corrective action;
- Identity of the account and the privileged user involved; and,
- The system processes involved.

Privileged users must not have permission to erase logs or de-activate logging of their own activities.

1.4.3 b) Independent review

Information Custodians must have a documented process to ensure that activity of privileged users is independently reviewed. Reviews must be conducted regularly and at random with the frequency being commensurate with the criticality, value and sensitivity of system and information assets. Following verification of logs, the individual checking them should digitally sign them and store or archive them securely in accordance with the approved records retention schedule. The audit logs must be reviewed prior to being discarded or overwritten.

Recommended Tests:

Note: 1.4.3 is reported on as part of the annual information security review.

- Demonstrate privileged user logs are independently reviewed.
- Demonstrate that controls protect against tampering or unauthorized changes to log information.
- Demonstrate logs are reviewed prior to discarding or overwriting.

1.4.4	**Faults must be logged, analyzed and appropriate action taken.** **a) Reporting and logging faults** **b) Analysis, resolution and corrective action**

Purpose: ***To support system security by establishing processes for reporting, logging, analyzing, resolving and correcting system faults.***

1.4.4 a) Reporting and logging faults

Information Owners and Information Custodians must implement processes for monitoring, reporting, logging, analyzing and correcting system faults reported by users and automated detection systems.

Fault logging requirements should be determined through a Security Threat and Risk Assessment and Privacy Impact Assessments.

Fault management reports must include:

- Description of fault including date, time, location and extent of fault;
- Analysis of probable source and cause;
- Actions taken to respond to and resolve the fault; and,
- Corrective action taken.

1.4.4 b) Analysis, resolution and corrective action

Information Custodians must review fault logs to ensure that faults have been resolved and documented in a fault management report. Information Custodians must provide the fault management report to Information Owners.

Analysis and corrective action includes:

- Defining the fault and probable cause(s);
- Assessing the effectiveness of corrective action(s);
- Checking to ensure that corrective action has not introduced unforeseen vulnerabilities;
- Identifying trends so that corrective action makes increasingly effective use of resources while improving results;
- Recommending upgrades, replacement of components, software or other elements that create or cause faults;
- Improving fault detection and reporting to reduce the time between fault occurrence and taking corrective action;
- Measuring the exposure caused by the fault;
- Reporting on performance impact(s); and,
- Periodically re-assessing logging requirements.

Recommended Tests:

Note: 1.4.4 is not reported on as part of the annual information security review.

- Demonstrate system faults by Ministry per fiscal year are reported.
- Demonstrate faults that cause information security issues are identified on the annual Information Security Review with an appropriate action plan.
- Demonstrate analysis is being performed in order to identify potentially larger issues (e.g., trend analysis, financial impact).
- Demonstrate logging activities are commensurate with maintaining target level of risk.

1.4.5 Computer clocks must be synchronized for accurate reporting.
a) Synchronization
b) Checking and Verification

Purpose: ***To ensure the integrity of information system logs.***

1.4.5 a) Synchronization

System administrators must synchronize information system clocks to:

- the local router gateway; or,
- the Government approved clock host.

1.4.5 b) Checking and Verification
System administrators must confirm system clock synchronization:

- Following power outages or brownouts;
- As part of incident analysis and audit log review; and,
- At least semi-annually in conjunction with Daylight Savings Time.

Time discrepancies must be reported to OCIO Helpdesk, Customer Service Centre.
The clock hosts must be synchronized with a national time service such as the Government of Canada, National Research Council's Network Time Protocol server.

Recommended Tests:
Note: 1.4.5 is reported on as part of the annual information security review.

- Demonstrate system clock synchronization follows the government policies and standards.

1.5 Control of operational software

1.5.1 The implementation of software on operational information systems providing services must be controlled.
a) Software changes to operational information systems
b) Software implementation controls

Purpose: ***To prevent compromise of operational information systems providing services from unauthorized software installation.***

1.5.1 a) Software changes to operational information systems
Information Owners and Information Custodians must implement procedures to control software installation on operational information systems providing services to ensure that:

- Updates of operational information systems are planned, approved, impacts assessed, tested, logged and have a rollback plan;
- Operations employees and end users have been notified of the changes, potential impacts and if required have received additional training;
- New releases of software are reviewed to determine if the release will introduce new security vulnerabilities;
- Modifications to operational software are logged;
- The number of employees able to perform the updates is restricted and kept to a minimum;
- Development code or compilers are not present on operational information systems; and,
- Vendor supplied software is maintained at the supported level.

1.5.1 b) Software implementation controls:
Pre-Implementation
Before an updated or new information system is implemented into the operational environment, checks must be performed to ensure that:

- A Security Threat and Risk Assessment has been carried out;
- A Privacy Impact Assessment has been performed and approved;
- Limitations of security controls are documented;
- Performance and capacity requirements can be met and support organizations have the capacity to maintain the information system;

- Development problems have been resolved successfully;
- The effects on existing operational information systems are known;
- Arrangements for fall-back have been established if the updated or new information system fails to function as intended;
- Error recovery and restart procedures are established;
- Business continuity plans are developed or updated;
- Operating procedures are tested;
- Changes are communicated to users who may be affected by the change;
- Users are educated to use the information system correctly and securely; and,
- Computer operators and system administrators are trained in how to run the information system correctly and securely.

Implementation
The installation process must include:

- Validating the load or conversion of data files;
- Installing executable code only, and not source code;
- Providing ongoing technical support;
- Implementing new or revised procedures and documentation;
- Discontinuing old software, procedures and documentation;
- Arranging for fall-back in the event of failure;
- Informing the individuals involved of their roles and responsibilities;
- Transferring responsibility for the information system from development teams to operational teams to ensure segregation of duties; and,
- Recording installation activity.

Post-implementation
Post-implementation reviews must include:

- The efficiency, effectiveness and cost of security controls;
- Lessons learned and scope for improvements of security controls; and,
- Security incidents and mitigation.

Recommended Tests:
Note: 1.5.1 is reported on as part of the annual information security review.

- Demonstrate a Security Threat and Risk Assessment and Privacy Impact Assessment have been completed.
- Demonstrate that the updating of software is implemented by trained administrators only after receiving appropriate authorization from management.
- Demonstrate software is only implemented after exhaustive testing.
- Demonstrate that before any introduction of software to systems, the implementation plan has a rollback strategy.
- Demonstrate an audit log is maintained of all updates and changes to software.

1.5.2 Systems documentation must be protected from unauthorized access.
a) Protection of systems documentation

Purpose: ***To prevent unauthorized access to sensitive information contained in systems documentation.***

1.5.2 a) Protection of systems documentation

Information Custodians and Information Owners must ensure that documented procedures for the secure use and storage of systems documentation are established and followed. Procedures must:

- Require information classification labelling of system documentation;
- Establish lists of users authorized to access system documentation on a 'need to know' basis;
- Establish handling rules for the information regardless of storage media (e.g., electronic, paper);
- Require use of access controls, passwords, encryption or digital signatures as appropriate to the information classification; and,
- Include a compliance monitoring process.

Recommended Tests:

Note: 1.5.2 is not reported on as part of the annual information security review.

- Demonstrate documented procedures for the secure use and storage of systems documentation are followed.

1.6 Technical vulnerability management

1.6.1	**Assessments for known exposures must be conducted to evaluate information system vulnerabilities and the management of associated risks.** **a) Vulnerability response processes**

Purpose: ***To mitigate damage to government operations resulting from exploitation of published vulnerabilities.***

1.6.1 a) Vulnerability response processes

Vulnerabilities which impact government information systems must be addressed in a timely manner to mitigate or minimize the impact on government operations. Information Custodians must establish processes to identify, assess and respond to vulnerabilities that may impact information systems by:

- Monitoring external sources of information on published vulnerabilities;
- Assessing the risk of published vulnerabilities;
- Testing and evaluating options to mitigate or minimize the impact of vulnerabilities;
- Applying corrective measures to address the vulnerabilities;
- Completing a Security Threat and Risk Assessment to verify the risk has been mitigated; and,
- Reporting to the Chief Information Security Officer on progress in responding to vulnerabilities.

Responsibilities for vulnerability response by service providers must be included in external party service agreements.

The Chief Information Security Officer must:

- Evaluate vulnerabilities and provide advice on appropriate government responses;
- Monitor progress in responding to vulnerabilities;
- Publish summary reports on vulnerability response activities and costs; and,
- When required, initiate incident response processes to address vulnerabilities.

Recommended Tests:

Note: 1.6.1 is reported on as part of the annual information security review.

- Demonstrate identified roles and responsibilities are established for the coordination of vulnerability management.
- Demonstrate emergency procedures for high risk vulnerabilities (e.g., Heartbleed, Shellshock) are documented and followed.
- Demonstrate patches are well tested prior to implementation.
- Demonstrate all vulnerability patches are actively logged.
- Demonstrate a priority patching criteria based on risk is established to address the most critical applications and information systems first.

1.6.2 Review of the rules governing the installation of software by employees must be established and implemented.
a) Restrictions on software installation

Purpose: ***To limit the installation of software to authorized employees to avoid security incidents.***

1.6.2 a) Restrictions on software installation
Uncontrolled installation of software on computing devices can lead to introducing vulnerabilities and then to information leakage, loss of integrity or other information security incidents, or to violation of intellectual property rights. Employees must receive authorization prior to installing software on government devices. Software installation must be consistent with the requirements of the Appropriate Use Policy.

Recommended Tests:
Note: 1.6.2 is reported on as part of the annual information security review.

- Demonstrate employees are made aware of acceptable/appropriate use policies.

1.7 Information systems audit considerations

1.7.1 Audit requirements and activities involving checks on operational systems must be planned and approved to minimize disruption to business processes.
a) Management of information systems compliance checking

Purpose: ***To prevent compliance checking activities from causing unplanned disruptions to operational information systems.***

1.7.1 a) Management of information systems compliance checking
Prior to commencing compliance checking activities such as audits, risk and controls reviews, monitoring or security reviews of operational information systems, the Manager responsible for the compliance checking activity, Information Owners and Information Custodians must define, document and approve the activities by:

- Determining the scope, duration and level of detail of the compliance checking activity;
- Limiting access rights to operational information systems for compliance checking employees to “read only”;
- Determining handling requirements for copies of files made by compliance checking employees including:
    - Establishing a separate environment for the analysis of files,
    - Restricting access to those files,

    - Logging the accesses made to those files, and,
    - Erasing files at the conclusion of compliance checking activities unless needed to support report findings;
- Identifying special testing or processing which may impact the operational information system (e.g., penetration tests, server vulnerability assessments) and by:
    - Notifying the Chief Information Security Officer prior to compliance checking activities to prevent triggering false security alarms from the infrastructure, and,
    - Scheduling tests to minimize disruption;
- Submitting the reports of penetration tests or vulnerability assessments to the Chief Information Security Officer immediately upon receipt; and,
- Requiring that employees conducting compliance checking activities maintain a segregation of duty from the operational information systems being checked.

Guidance for compliance checking activities can be obtained from the Information Security Branch, Office of the Government Chief Information Officer.

Recommended Tests:
Note: 1.7.1 is reported on as part of the annual information security review.

- Demonstrate regular audit requirements timing and scope are agreed upon to minimize disruption.
- Demonstrate there is a clear segregation of duties between the auditor and operational employees.
- Demonstrate all access is monitored and logged.

1.7.2 Access to system audit tools must be controlled to prevent misuse or compromise.
a) Protection of information system audit tools

Purpose: ***To minimize risks to information and information systems from inappropriate use of audit tools.***

1.7.2 a) Protection of information system audit tools
Managers responsible for compliance checking activities and Information Custodians must control the use of audit tools by:

- Restricting access to authorized employees who have a need-to-know;
- Installing or enabling specialized audit tools for the duration required by the compliance checking activity;
- Removing information system access at the conclusion of the compliance checking activities; and,
- Notifying the Chief Information Security Officer prior to the use of audit tools.

Recommended Tests:
Note: 1.7.2 is not reported on as part of the annual information security review.

- Demonstrate the use of audit tools is authorized.