BRITISH COLUMBIA | Ministry of Citizens' Services

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE 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 System Acquisition, Development and Maintenance

This chapter establishes requirements for incorporating security measures into the life-cycle of an information system. Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.

Information security is integrated into the creation, modification, implementation and expansion by ongoing security practices such as the management of vulnerable points and securing system files. For applications, information security can be applied to the validation of data input and output and by encoding information using electronic keys.

1.1 Security requirements of information systems

1.1.1	**Security controls must be identified as part of the business requirements for new information systems or enhancements to existing information systems.** **a) Security requirements for information systems** **b) Security requirements at implementation**

Purpose: ***To integrate system security requirements into business processes supporting the development, maintenance and acquisition of information systems.***

1.1.1 a) Security requirements for information systems

Information Owners must conduct a Security Threat and Risk Assessment and a Privacy Impact Assessment during the requirements phase when developing, implementing major changes to, or acquiring an information system, to:

- Identify the security requirements necessary to protect the information system; and,
- Assign a security classification to the information and the information system.

The Information Owner must ensure that information system development or acquisition activities are done in accordance with documented requirements, standards and procedures which include:

- Testing the information system to verify that it functions as intended;
- Enforcing change control processes to identify and document modifications or changes which may compromise security controls or introduce security weaknesses; and,
- Using common government processes and services (e.g., authentication, access control, financial management).

1.1.1 b) Security requirements at implementation

Information Owners and Information Custodians must ensure that sufficient controls are in place to mitigate the risk of information loss, error or misuse from information systems. Prior to implementation, information systems must be assessed to verify the adequacy of, and document the details of, the security controls used, by completing a security certification.

Different tiers of applications need to be separated across different platforms or servers (e.g., web interface must be on a different server from the data base).

Information systems should have a documented and maintained System Security Plan. The Plan should include:

- A summary of risks identified in the Security Threat and Risk Assessment;
- Results of the system certification;
- Roles and responsibilities for information system security management;
- Specific procedures and standards used to mitigate risks and protect the information system;
- Communication procedures for security-relevant events and incidents; and,
- Monitoring procedures.

While Security Threat and Risk Assessments are not required for all apps on mobile devices, where the app is used for processing government information, a Security Threat and Risk Assessment and Privacy Impact Assessment must be completed before the use of the app. Apps should be downloaded only from official vendor provided app stores. Mobile devices attached to the government network must be used according to vendor specifications (e.g., not removing vendor built-in restrictions).

Employees should always consider potential risks before downloading apps on their mobile devices. Some apps have been found to have harmful effects and may inadvertently release information from the mobile device to third parties.

Recommended Tests:

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

- Demonstrate information security requirements are derived from compliance requirements in information security policies, guidelines and regulations.
- Demonstrate a Privacy Impact Assessment has been completed for all information systems with personal information.
- Demonstrate users and operators have a clear understanding of roles and responsibilities.

1.1.2	**Information in application services information systems must be protected from fraudulent activity, contract dispute, unauthorized disclosure and modification.** **a) Electronic commerce** **b) Electronic documents**

Purpose: ***To enable secure electronic commerce for the delivery of government services.***

1.1.2 a) Electronic commerce

Prior to initiating or implementing electronic commerce information systems, Information Owners and Information Custodians must:

- Ensure that the Security Threat and Risk Assessment is conducted and addresses threats and risks related to electronic commerce;
- Confirm that a Privacy Impact Assessment has been conducted and approved;
- Determine the security classification of the information and information system(s) involved;
- Ensure that the user notification and acceptance of terms and conditions of use complies with government policies and standards;
- Ensure multi-factor authentication is used commensurate with the sensitivity and value of the information;
- Develop and implement processes to maintain content currency;

- Confirm the information system has received security certification and accreditation; and,
- Develop Business Continuity Plans and supporting Disaster Recovery Plans.

1.1.2 b) Electronic documents

When accepting or submitting electronic documents, Information Owners and Information Custodians must:

- Authenticate the users claimed identity;
- Determine an authorization process for approving contents, issue or sign key documents;
- Determine the requirements for confidentiality, integrity, proof of dispatch and receipt of key documents and the confidentiality of contracts; and,
- Ensure the protection requirements of any confidential information.

Recommended Tests:

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

- Demonstrate applied authorization and authentication when providing services over networks.
- Demonstrate the level of protection for payments (e.g., Payment Card Industry standards).
- Demonstrate procedures for ensuring confidentiality.

1.1.3	**Information systems utilizing on-line transactions must have security controls commensurate with the value and sensitivity of the information.** **a) On-line transaction security** **b) Payment card transaction security**

Purpose: ***To maintain the confidentiality, integrity and availability of on-line transactions in information systems.***

1.1.3 a) On-line transaction security

Information Owners and Information Custodians are responsible for ensuring information systems containing on-line transactions have implemented security controls commensurate with the value and sensitivity of the information.

Security controls must be implemented to prevent incomplete transmission, misrouting, repudiation of transaction, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication and replay. Security controls include:

- Validating and verifying user credentials;
- Using digital signatures;
- Using cryptography to protect data and information;
- Establishing secure communications protocols; and,
- Storing on-line transaction details on servers within the appropriate network security zone.

1.1.3 b) Payment card transaction security

Information Owners and Information Custodians are responsible for ensuring that information systems used for processing payment card transactions, or connected to payment card transaction processing systems, comply with the Payment Card Industry Data Security Standard.

The Payment Card Industry Data Security Standard V3.0 has 12 high-level requirements:

- Install and maintain a firewall configuration to protect cardholder data;
- Do not use vendor-supplied defaults for system passwords and other security parameters;

- Protect stored cardholder data;
- Encrypt transmission of cardholder data across open, public networks;
- Protect all systems against malware and regularly update anti-virus software or programs;
- Develop and maintain secure systems and applications;
- Restrict access to cardholder data by business need-to-know;
- Identify and authenticate access to system components;
- Restrict physical access to cardholder data;
- Track and monitor all access to network resources and cardholder data;
- Regularly test security systems and processes; and,
- Maintain standards and policies that addresses information security for all employees.

Recommended Tests:

Note: 1.1.3 is reported on as part of the annual information security review.

- Demonstrate that storage of transaction details is located outside any publicly accessible environment.
- Demonstrate security controls are commensurate with the classification of the information that is being protected.

1.2 Security in development and support process

1.2.1	**Policies, standards, and guidelines for the development of software and systems must be established and applied to developments within the organization.** **a) Secure development process** **b) Secure programming techniques**

Purpose: ***To ensure that information security is designed and implemented within the development life-cycle of information systems.***

1.2.1 a) Secure development process

Information Owners and Information Custodians must ensure that software and systems developed internally follow established policies, standards and best practices for secure development process. The established policies and standards must be applied consistently to all developments within the organization.

A secure development process is a necessity in developing a secure information system. Within a secure development life-cycle of information systems, the following aspects must be considered:

- Security of the development environment;
- Security in the software development methodology;
- Secure coding guidelines for each programming language used;
- Inclusion of security requirements starting from the design phase;
- Security checkpoints within the development milestones;
- Secure repositories;
- Security in the version control and updates;
- Required application security knowledge; and,
- Developer capability of avoiding, finding and fixing vulnerabilities.

1.2.1 b) Secure programming techniques

Secure programming techniques must be used both for new developments and in code re-use scenarios where the standards applied to development may not be known or are not consistent with current best practices. Secure coding standards must be considered and where relevant mandated for use.

- Program code must not be altered unless authorized to do so;
- Any variations to program code must be documented; and,
- All changes to existing code must ensure applicable standards have been applied for program security.

If development is outsourced, the organization must obtain assurance that the external party complies with the policies for secure development.

Recommended Tests:

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

- Demonstrate security requirements were defined in the design phase.
- Demonstrate security in version control.
- Demonstrate developer capability in identifying and addressing vulnerabilities.
- Demonstrate a Privacy Impact Assessment has been completed for all software.

1.2.2 Changes to software must be controlled by the use of formal change control procedures.
a) Changes to software during information systems development
b) Changes to software for operational information systems

Purpose: To ensure that information systems are not compromised from changes to software.

1.2.2 a) Changes to software during information systems development

Information Owners must implement a change control process during development which includes:

- Requiring that change requests originate from authorized employees;
- Requiring that proposed changes are reviewed and assessed for impact; and,
- Logging all requests for change.

1.2.2 b) Changes to software for operational information systems

Information Owners must implement a change control process during the maintenance phase including:

- Requiring that change requests originate from authorized employees;
- Performing an impact assessment considering items such as the System Security Plan and proposed modifications;
- Documenting fallback plans;
- Documenting approval of changes proposed prior to the commencement of the work;
- Documenting the acceptance tests and approval of the results of acceptance testing;
- Updating the System Security Plan and other system, operations and user documentation with the details of changes in accordance with records management policy;
- Maintaining version control for all changes to the software; and,
- Logging all requests for change.

Recommended Tests:

Note: 1.2.2 is reported on as part of the annual information security review.

- Demonstrate there is an authorization process and scheduled procedures are followed.

- Demonstrate all software is thoroughly tested prior to implementation.
- Demonstrate that there was a change control procedure for changes to the application(s) that included a means to back-out, changes were pre-approved and authorized, and all documentation has been properly updated.
- Demonstrate there is a version control for all software updates.

1.2.3 Information systems must be reviewed and tested when operating system changes occur.
a) Changes to the operating system

Purpose: To ensure information systems will not be disrupted or compromised.

1.2.3 a) Changes to the operating system

Information Custodians must notify information system Information Owners and other affected parties of operating system changes to allow:

- Sufficient time for the review and testing of information systems prior to implementation;
- Review of System Security Plans to ensure information systems will not be compromised by the change;
- Significant changes to the operating system must have a completed Security Threat and Risk Assessment completed;
- Information system testing with the changes to the operating system in a separate (i.e., test) environment; and,
- Update of business continuity plans if required.

Recommended Tests:

Note: 1.2.3 is reported on as part of the annual information security review.

- Demonstrate application control and integrity procedures to ensure that security has not been compromised by changes to the platform.
- Demonstrate that notification of platform changes permit adequate time for appropriate testing prior to implementation.
- Demonstrate the business continuity plan has been updated to reflect platform changes.
- Demonstrate platforms with personal information processing have a completed Privacy Impact Assessment.

1.2.4 Modification of commercial-off-the-shelf software is limited to essential changes that are strictly controlled and documented.
a) Modifying commercial-off-the-shelf software
b) Applying vendor supplied patches and updates

Purpose: To reduce the risk of information system functionality loss.

1.2.4 a) Modifying commercial-off-the-shelf software

Other than vendor supplied patches, commercial-off-the-shelf (COTS) software must not be modified except in exceptional circumstances when needed for a critical business requirement. This requirement must be documented and approved by the Information Owner and Information Custodian.

If changes to COTS software are required, the Information Owners and Information Custodians must determine:

- The effect the change will have on the security controls in the software;
- If consent of the vendor is required;
- If the required functionality is included in a new version of the software;
- If government will become responsible for maintenance of the software as a result of the change; and,
- Compatibility with other software in use.

If changes are made to COTS software the original software must be kept unaltered and the changes must be:

- Logged and documented, including a detailed technical description;
- Applied to a copy of the original software; and,
- Tested and reviewed to ensure that the modified software continues to operate as intended.

1.2.4 b) Applying vendor supplied patches and updates

A software update management process must be maintained for commercial-off-the-shelf (COTS) software to ensure:

- The most up-to-date approved patches have been applied; and,
- The version of software is vendor supported.

Recommended Tests:

Note: 1.2.4 is reported on as part of the annual information security review.

- Demonstrate a copy of the unmodified software is retained.
- Demonstrate a software management program is in place to ensure software patching is up-to-date.
- Demonstrate all changes to software are thoroughly tested prior to implementation.

1.2.5 Principles for engineering secure systems must be established, documented, maintained and applied to any information system implementation efforts.
a) Secure engineering principles
b) Outsourcing engineering security
c) Application development

Purpose: ***To ensure information security is designed in all architectural layers of information systems.***

1.2.5 a) Secure engineering principles

Information Owners and Information Custodians must establish and document secure information system engineering procedures based on security engineering principles and best practices. The procedures must be applied to all in-house information system engineering activities. Security must be designed into all architecture layers (business, data, applications and technology) balancing the need for information security with the need for accessibility. New technology must be analyzed for security risks and the design must be reviewed against known attack patterns.

Secure engineering procedures must be reviewed regularly to ensure they remain current to reflect the changes in the environment and threat landscape.

1.2.5 b) Outsourcing engineering security

Information Owners and Information Custodians must ensure that contracts and other binding agreements incorporate the secure engineering principles and procedures for outsourced information systems.

1.2.5 c) Application development

Application development procedures must apply secure engineering techniques in the development of applications that have input and output interfaces and provide guidance on user authentication techniques, secure session control and data validation, sanitization and elimination of debugging codes.

Recommended Tests:

Note: 1.2.5 is reported on as part of the annual information security review.

- Demonstrate information systems engineering is based on security engineering principles that are documented and are applied.
- Demonstrate new technologies are analyzed for security risks.
- Demonstrate new technology designs are reviewed against known attack patterns.

1.2.6 Organizations must establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development life-cycle.
a) Secure development environment

Purpose: ***To ensure the security of information during the development and system integration process.***

1.2.6 a) Secure development environment

A secure development environment includes people, processes and technologies associated with system development and integration. Information Owners and Information Custodians must assess the risks associated with individual system development efforts and establish secure development environments for system development, considering:

- Sensitivity of data to be processed, stored or transmitted by the system;
- Applicable external and internal requirements (e.g., from regulations, policies and standards);
- The need for segregation between different development environments;
- Security controls already in place that support system development;
- Trustworthiness of employees working in the environment;
- The degree of outsourcing associated with system development;
- Control of access to the development environment;
- Monitoring of changes to the environment and code stored therein;
- Backups are stored at secure offsite locations; and,
- Control over movement of data from and to the environment.

Once the level of protection is determined for a specific development environment, Information Owners and Information Custodians must document corresponding processes in secure development procedures and provide these to all individuals who need them.

Personal information must not be used in the testing or development phases without a valid policy exemption from the Office of the Chief Information Officer.

Recommended Tests:

Note: 1.2.6 is reported on as part of the annual information security review.

- Demonstrate that all applicable regulations and standards are considered in the development phase.
- Demonstrate segregation between development, test and operational environments.
- Demonstrate that security is considered throughout each step of the system development life-cycle.
- Demonstrate employees involved with the systems development are made aware of system development security.

1.2.7 Controls must be applied to secure outsourced information system development.
a) Outsourced information system development

Purpose: To ensure information systems perform as expected and meet security requirements.

1.2.7 a) Outsourced information system development

Information Owners and Information Custodians must consider the following when outsourcing information system development:

- Procurement policy for licencing, ownership and intellectual property rights;
- Escrow arrangements in the event of the failure of the external party;
- Testing of the information system for common vulnerabilities and malicious code;
- Rights of access for audit and certification of the quality and accuracy of the work; and,
- Contractual requirements for quality and security functionality of the information system.

Information Owners and Information Custodians must ensure that the outsourced information system meets the requirements defined in the system development agreements.

Recommended Tests:

Note: 1.2.7 is reported on as part of the annual information security review.

- Demonstrate identification of ownership in outsourcing software development.
- Demonstrate that intellectual property rights are managed through licencing agreements.
- Demonstrate audit access is stipulated in procurement contracts.
- Demonstrate information system security is involved in every step of outsourced development.

1.2.8 Testing of security functionality must be carried out during development.
a) Testing during development

Purpose: To ensure that security functionality is carried out during the development process.

1.2.8 a) Testing during development

Information Owners and Information Custodians must ensure that new and updated systems undergo thorough testing and verification during the development processes. A detailed schedule of test activities, inputs and expected outputs under a range of conditions must be prepared as part of testing and verification processes.

Independent acceptance testing must be undertaken to ensure that the system works as expected and only as expected. The extent of testing must be in proportion to the importance and nature of the system.

Recommended Tests:
Note: 1.2.8 is reported on as part of the annual information security review.

- Demonstrate all new and updated systems are tested prior to implementation.
- Demonstrate acceptance testing is segregated from development.

1.2.9 Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance.
a) System acceptance process
b) System acceptance criteria
c) Security certification
d) System accreditation

Purpose: ***To ensure that new or upgraded information systems are tested against defined, agreed and documented criteria for acceptance, prior to becoming operational.***

1.2.9 a) System acceptance process
Information Owners must ensure that system acceptance criteria are defined as part of the system development and acquisition process.

Prior to implementing new or upgraded information systems, Information Owners and Information Custodians must ensure:

- Acceptance criteria are identified including privacy, security, systems development and user acceptance testing;
- Security certification is attained, indicating the system meets minimum acceptance criteria; and,
- Security accreditation to proceed with implementation is attained.

A Privacy Impact Assessment must be completed for new or upgraded information systems.

1.2.9 b) System acceptance criteria
Information Owners and Information Custodians must document system acceptance criteria, including:

- Projected performance and resource capacity requirements;
- Disaster recovery, restart, and contingency plans and procedures;
- Impact on standardized routine operating procedures and manual procedures;
- Implementation of security controls;
- Assurance that installation of the new system will not adversely affect existing systems, particularly at peak processing times;
- Business continuity arrangements;
- Training requirements; and,
- User acceptance testing.

1.2.9 c) Security certification
The Information Owners and Information Custodians must receive assurance that a new or updated information system meets minimum security acceptance criteria.

Assurance should be obtained by conducting either an independent Security Threat and Risk Assessment or a Risk and Controls Review which determines whether a system includes adequate controls to mitigate security risks. This process will also determine the effect of the new system on the overall security of government information systems.

1.2.9 d) System accreditation
Information Owners and Information Custodians must authorize the implementation of new or upgraded information systems based on the degree to which the acceptance criteria are satisfied.

Recommended Tests:
Note: 1.2.9 is reported on as part of the annual information security review.

- Demonstrate that the criteria for acceptance are identified during the procurement phase.
- Demonstrate Privacy Impact Assessments are completed prior to acceptance.
- Demonstrate that all acceptance tests are documented.

1.3 Correct processing in applications

1.3.1 Data input to an information system must be validated to ensure that it is correct and appropriate.
a) Input data validation

Purpose: ***To maintain the integrity of information in information systems by preventing the introduction of invalid or incomplete data.***

1.3.1 a) Input data validation
Information Owners must ensure the validity and integrity of data input to information systems by:

- Limiting fields to accept specific ranges of data (e.g., defining out of range values or upper and lower data volume limits);
- Checking for invalid characters in data fields;
- Making key fields mandatory;
- Verifying the plausibility of input data using business rules;
- Protecting against common attacks (e.g., buffer overflows); and,
- Using control balances to verify complete input and processing.

1.3.2 Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity.
a) Internal processing

Purpose: ***To prevent errors, loss, unauthorized modification or misuse of information in information systems.***

1.3.2 a) Internal processing
Information Owners must require that information systems include internal processing checks to:

- Detect unauthorized or incorrect changes to information;
- Prevent information from being accidentally overwritten;

- Prevent internal information from being disclosed via information system responses;
- Protect against common attacks (e.g., buffer overflows);
- Check the integrity, authenticity or any other security feature of data or software downloaded or uploaded between central or remote computers;
- Maintain audit trails; and,
- Provide error and exception reports.

Information Owners must ensure that error and exception reports are monitored, followed up and signed off on a regular basis.

1.3.3 Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content.
a) Message integrity

Purpose: ***To prevent errors, loss, unauthorized modification or misuse of information in information systems.***

1.3.3 a) Message integrity

Information Owners must determine message integrity requirements during the requirements definition phase of system development or acquisition.

1.3.4 Data output from an information system must be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.
a) Output data validation

Purpose: ***To verify correct information processing for output data.***

1.3.4 a) Output data validation

Information Owners must require that processes are documented to validate the data output from an information system by:

- Reconciling control balances to verify that data is processed accurately;
- Verifying the plausibility of output data using business rules;
- Providing sufficient information for a reader or subsequent information system to determine the accuracy, completeness, precision and classification of the information;
- Maintaining audit trails; and,
- Providing error and exception reports.

Information Owners must ensure that error and exception reports are monitored, followed up and signed off on a regular basis.

1.4 Test data

1.4.1	**Test data must be protected and controlled using the same procedures as for data from operational information systems.** **a) Protection of test data**

Purpose: ***To protect information from unauthorized access or use.***

1.4.1 a) Protection of test data

Information Owners must implement procedures to ensure that:

- Using test data extracted from operational information systems is authorized and logged to provide an audit trail;
- Test data is protected with controls appropriate to the security classification of the information and information system; and,
- Data from operational information systems is removed from the test environment once testing is complete.

Sensitive or personal information from operational information systems should not be used as test data. Where personal or sensitive data must be used for testing purposes, sensitive details and content should be removed, depersonalized or de-identified.

In rare cases when sensitive or personal data from operational systems has to be used for testing purposes, the following conditions must be met:

- Information Owners must provide a strong business case for the use of operational data containing sensitive or personal data for testing purposes;
- Privacy Impact Assessment and Security Threat and Risk Assessment must be completed specific to the use of operational data in test;
- Use of production data for testing purposes must be approved by the program area Executive Director and Ministry Chief Information Officer;
- Testing with the use of operational data must occur only in a production-like environment;
- The data to be used for testing purposes in the production-like environment must be handled with the same care and diligence as in the production environment with the same or more stringent security controls;
- Access to test data must be limited to the minimum number of individuals required to perform testing activities and must be based on clearly defined roles and responsibilities, and formal approval process;
- Information Owners must ensure that access to sensitive or personal information used for testing is monitored and reviewed on a regular basis to detect inappropriate or unauthorized access attempts, at a minimum once a week;
- Where sensitive or personal information is used, Information Owners must ensure that only information fields necessary for testing be used (e.g., if successful results can be achieved using the last four digits of a Social Insurance Number, avoid using the whole number);
- Information Owners must ensure that the smallest subset of sensitive or personal information is used, which is necessary to complete the testing (e.g., if successful results can be achieved using a small number of records, avoid using the whole dataset);
- After testing activities are completed, Information Owners must ensure that test data is erased from the production-like environment in accordance with government standards;
- Information Owners must maintain detailed project documentation on testing activities and processes for audit purposes, including a list of employees involved in testing, date and time

when testing began and ended, any deviations from the established processes or procedures that may affect the existing security controls, and any other relevant information; and,

- The documentation must demonstrate why the use of sensitive or personal information is necessary.

Information Owners must ensure that the use of personal information for testing purposes does not contravene the requirements of the Freedom of Information and Protection of Privacy Act. Privacy, Compliance and Training Branch in the Ministry of Finance manages privacy for the Province and should be consulted when test data involves personal information.

Guidelines:
Output from test systems should be labelled “test”.

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

- Demonstrate that testing requires production data and cannot be done reliably otherwise.
- Demonstrate controls applied to test data are appropriate for the security classification of the information or the information system.
- Demonstrate personal or sensitive data is depersonalised or removed prior to its use in test, unless it is required.
- Demonstrate evidence of authorization approvals for use of operational data in test systems.
- Demonstrate architecture documentation that details what access controls exist on test systems.