BRITISH COLUMBIA | Ministry of Citizens' Services

SUPPLIER RELATIONSHIPS AND CLOUD COMPUTING 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 Supplier Relationships

This chapter covers the requirements for information security in supplier agreements. These are important to consider in outsourcing deals, awarding contracts and in IT procurement services.

1.1 Information security in supplier agreements

1.1.1 Identified security requirements must be addressed, agreed upon and documented prior to granting external parties access to information, information systems or information processing facilities.
a) Security requirements

Purpose: ***To ensure that risks associated with external party access to information and information systems have been mitigated by applying security controls as determined by business needs.***

1.1.1 a) Security requirements

Prior to granting access to non-public information and information systems for external parties Information Owners and Information Custodians must:

- Determine that mitigation strategies have been implemented to address security requirements;
- Review the Security Threat and Risk Assessment for asset protection requirements including:
  - Asset classification,
  - Legislative, regulatory, standards and policy considerations, and,
  - Intellectual property rights obligations;
- Complete a Privacy Impact Assessment;
- Determine that security controls will not adversely affect target service levels; and,
- Document the roles and responsibilities of the Information Owner, Information Custodian and the external party in a formal agreement.

Recommended Tests:

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

- Demonstrate system security requirements for external party access to government information assets are documented.
- Demonstrate there is a formal agreement for external party access to non-public information.

1.1.2 External party access to information, information systems or information processing facilities must be based on a formal contract containing necessary information security requirements.
a) External party access agreements
b) Security requirements
c) Service level continuity

Purpose: ***To ensure external parties accessing information assets and information processing facilities are required to implement and use security controls.***

1.1.2 a) External party access agreements
Information Owners and Information Custodians must ensure access to information assets and information processing facilities by external parties is only provided after an access agreement has been completed and signed.

Access agreements must include:

- Roles and responsibilities of the Information Owner, Information Custodian and the external party;
- Non-disclosure agreements;
- Sub-contracting requirements;
- Specialized security controls (i.e., meet particular business and security arrangements, legal or regulatory requirements);
- Conditions for contract termination;
- Audit and compliance monitoring rights, responsibilities and processes;
- Reporting obligations for suspected or actual security and privacy incidents;
- Renewal and extension conditions; and,
- Requirements for regular compliance reviews.

Approved forms of agreement include:

- General Service Agreement for purchase of goods or services;
- Agreements for Alternate Service Delivery or Public Private Partnership;
- Information Sharing Agreement; or,
- Other forms of agreement as approved by Legal Services.

1.1.2 b) Security requirements
Information Owners and Information Custodians must ensure the security requirements of external party access agreements include:

- Notification of obligations of the parties to adhere to legislation and regulation;
- Requirements to adhere to agreed information security policies and procedures;
- Processes for amending the agreement;
- Acknowledgement by the external party that ownership of information is retained by the Province;
- Confidentiality obligations of the external party and their employees or agents;
- Requirements for use of unique user identifiers;
- Processes for conducting audits and compliance monitoring activities;
- Responsibilities and processes for reporting security and privacy incidents; and,
- Assurances that disciplinary action will be applied to employees or contractors who fail to comply with the terms of the agreement.

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

- Demonstrate third-party access agreements are in place prior to granting access.

1.1.3 Agreements with suppliers must include requirements to address the information security risks involving or associated with information and communications technology components, services and product supply chain.

a) Supplier agreement considerations

Purpose: ***To identify security controls concerning supply chain security in supplier agreements.***

1.1.3 a) Supplier agreement considerations
Information Owners and Information Custodians must identify the security risks concerning the supplier chain relationships and specify the necessary controls in the agreements.

Supply chain risk management practices should be built on top of general information security, quality, project management and system engineering practices but do not replace them. Information Owners and Information Custodians must work with suppliers to understand their supply chain and any matters that have an impact on the products and services being provided. Agreements with suppliers must address the security requirements that involve other suppliers in the supply chain. Supply chain as addressed here includes cloud computing services.

The following security controls must be considered for inclusion in supplier agreements concerning supply chain security:

- Defining information security requirements that apply to information systems and information technology product or service acquisitions;
- Requiring that suppliers apply government security requirements throughout their supply chain if the services are further subcontracted as a whole or in part;
- Requiring that suppliers apply appropriate security practices throughout the supply chain for products that include components purchased from other suppliers;
- Implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;
- Implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;
- Obtaining assurance that critical components and their origin can be traced throughout the supply chain;
- Obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;
- Defining the rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers; and,
- Implementing specific processes for managing information and communication technology component life-cycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

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

- Demonstrate a review of controls in supplier agreements.
- Demonstrate supplier life-cycle management.
- Demonstrate a monitoring process for supplier agreements.
- Demonstrate contingencies for supplier disruption of services.

1.2 Supplier service delivery management

1.2.1	**Prior to using external information and technology services, security controls, service definitions and delivery levels must be identified and included in the agreement with the external party.** **a) Identifying security requirements in procurement** **b) Service level continuity**

Purpose: ***To ensure service agreements with external parties specify requirements for security and service level continuity.***

1.2.1 a) Identifying security requirements in procurement

Information Owners and Information Custodians must include security requirements in procurement documents for information and information system services being delivered by external parties. Security requirements must be documented when:

- Drafting procurement documents (e.g., Request for Information, Request for Proposal);
- Evaluating bids to confirm acknowledgement and capability;
- Preparing agreements or contracts; and,
- Developing transition and fall back plans (e.g., migration from one service provider to another).

1.2.1 b) Service level continuity

Information Owners and Information Custodians must ensure supplier service agreements document service level continuity requirements and include processes for:

- Ongoing review of service level needs with business process owners;
- Audit and compliance monitoring rights and responsibilities;
- Communicating requirements to service providers;
- Obtaining periodic confirmation from service providers that adequate capacity is maintained;
- Reviewing the adequacy of the service provider’s contingency plans for responding to disasters or major service failures; and,
- Establishing the metrics for service delivery levels (including risk profiles and audit trigger levels).

Standards:

General Service Agreement and Schedule G

Recommended Tests:

Note: 1.2.3 is not reported on as part of the annual information security review.

- Demonstrate the procurement document includes the Security Schedule G.
- Demonstrate the procurement document addresses the service level continuity requirements.

1.2.2 Services provided by external parties must be regularly monitored and the reports and records reviewed.
a) Monitoring and review of external party services

Purpose: ***To ensure that services delivered by external parties maintain compliance with security and audit requirements.***

1.2.2 a) Monitoring and review of external party services

Information Owners and Information Custodians must establish processes to manage and review the information security of external party delivered services by:

- Assigning responsibility for monitoring to a designated employee;
- Maintaining an inventory of agreements and associated access rights;
- Monitoring for compliance through processes such as:
    - Conducting internal self-assessments of control processes,
    - Requiring external parties conduct and submit self-assessments,
    - Using embedded audit tools,
    - Requiring external parties to submit annual management assertions that controls are being adhered to,
    - Conducting independent security reviews, audits and updates to risk and controls reviews, and,
    - Analysis of audit logs;
- Establishing a process, jointly with the service provider, to monitor, evaluate, investigate and remediate incidents; and,
- Establishing performance measures within ministry service plans to ensure adequate service levels are maintained and measured.

Recommended Tests:

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

- Demonstrate reviews are conducted on third-party delivered services.
- Demonstrate there is a process to manage and review the information security of external party delivered services.
- Demonstrate service agreements identify frequency of audits.
- Demonstrate performance measures are established and that suppliers provide adequate service levels.
- Demonstrate management signs off on the completion of audit reviews.
- Demonstrate performance measures are established to ensure adequate service levels are maintained and measured.

1.2.3 Changes to the provision of services by suppliers for information system services must consider the criticality of the information systems, processes involved and re-assessment of risks.
a) Change management

Purpose: ***To ensure that changes to information system services delivered by external parties maintain or enhance security controls.***

1.2.3 a) Change management

Information Owners and Information Custodians must ensure agreements with external party service providers include provisions for:

- Amending agreements when required by changes to legislation, regulations, business requirements, policy or service delivery; and,
- Requiring the service provider to obtain pre-approval for significant changes involving:
    - Network services,
    - New technologies,
    - Use of new or enhanced system components (e.g., software or hardware),
    - System development, test tools and facilities,
    - Modification or relocation of the physical facilities, and,
    - Sub-contracted services.

Information Owners and Information Custodians must ensure the change management process for information systems services delivered by external parties includes, as required:

- Reviewing and updating the Security Threat and Risk Assessment to determine impacts on security controls;
- Implementing new or enhanced security controls where identified by the risk assessment;
- Reviewing and updating the Privacy Impact Assessment;
- Initiating and implementing revisions to policies and procedures; and,
- Revising employee awareness and training resources.

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

- Demonstrate the change management process for information systems services delivered by suppliers is included in the service agreements.
- Demonstrate organizational agreement allows for the organization to propose and implement changes to service agreements.
- Demonstrate all changes to services provided by the supplier were authorized prior to implementation.

1.2.4	**Assessment of risks from external party access to government information, information systems or information processing facilities must be undertaken, and appropriate security controls implemented.** **a) Risk assessment** **b) Risk mitigation and acceptance**

Purpose: ***To ensure the*** **risks** ***of external party access to information and information systems are identified, assessed, mitigated and managed.***

1.2.4 a) Risk assessment
Information Owners and Information Custodians are responsible for assessing the business requirements and associated risks related to external party access to information and information systems.

Risk assessments must be documented during the conceptual design phase of a project and updated throughout the life-cycle of the information system (e.g., prior to and following technical or business process changes to the information system).

The assessment of risks related to external party access must consider:

- If existing controls prevent external parties from accessing facilities or information that are not needed to meet the business requirements for the access;
- Impacts to the controls of the information processing facilities involved;
- The classification of the information assets;
- Policies and processes the external party has for employee hiring, training on security and privacy issues and incident reporting;
- Internal and external processes for managing and reporting security and privacy incidents;
- Processes for identifying, authorizing, authenticating and reviewing access rights of employees and systems of the external party;
- Security controls to be used by the external party when storing, processing, communicating, sharing or exchanging information;
- Impacts to both parties resulting from assets being unavailable; and,
- Data integrity requirements including impacts of accessing or using inaccurate information.

1.2.4 b) Risk mitigation and acceptance
Prior to authorizing access by external parties to information and information systems, Information Owners and Information Custodians must confirm that:

- A risk and controls review has been completed and identified risks have been mitigated or accepted;
- The terms and conditions of access are documented (e.g., services agreements, contracts, memoranda of understanding);
- Responsibilities for managing and monitoring the external party access have been assigned and documented; and,
- Security controls have been implemented and tested.

Recommended Tests:
Note: 1.2.4 is not reported on as part of the annual information security review.

- Demonstrate the risk assessment for external party access to government information has been documented.
- Demonstrate the risk assessment document has been updated throughout the life-cycle of the information system.

1.3 Cloud Computing

1.3.1 A comprehensive, documented policy on the use of cloud services must be produced and communicated to all individuals who require cloud services.
a) Cloud Computing Policy
b) Awareness requirements

Purpose: ***To ensure a consistent approach is followed regarding the procurement and use of cloud services.***

1.3.1 a) Cloud Computing Policy

Cloud computing relies on sharing resources rather than having local servers handle applications and storage. Cloud computing is a term used to describe on-demand resource pooling, rapid elasticity and measured services with broad network access (e.g., Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS)).

The Cloud Computing Policy is a documented corporate policy for the purchase and use of cloud services, which is:

- Based on the Office of the Chief Information Officer's strategy;
- Approved by executive management;
- Distributed to all relevant individuals throughout government; and,
- Applied throughout government.

Information Owners are responsible for determining the information security classification of the data to be moved to a cloud service and the security requirements in using cloud computing services.

Information Owners and Information Custodians must include the Office of the Chief Information Officer and the Chief Information Security Officer, or a designate, as part of the business functions (e.g., procurement and legal) for all cloud initiatives, and in the definition of standard and contractual requirements for the procurement and use of cloud services, to ensure that all controls and protection levels for cloud services have security by design.

1.3.1 b) Awareness requirements

Specific awareness activities must be performed to help ensure all employees:

- Are aware of the corporate policy on the use of cloud services; and,
- Are educated about the risks of using unapproved cloud services.

Recommended Tests:

Note: 1.3.1 is not reported on as part of the annual information security review.

- Demonstrate the use of cloud services follows government policy and standards.

11.3.2 Information Owners and Custodians are responsible for determining the appropriateness of using a cloud service.
a) Information Security Classification
b) Security of cloud services
c) Technical specifications

Purpose: ***To ensure a consistent approach is followed regarding the procurement and use of cloud services.***

1.3.2 a) Information Security Classification

Information Owners must first determine the security classification of the data to be transmitted, processed and/or held in the cloud before the data can be moved to the cloud. The information security classification of the data is assessed on whether the data contains personal information, its sensitivity, confidentiality and criticality to business operations (e.g., commercial information, intellectual property (IP), legal, regulatory and privileged information (LRP), logistical information, management information).

Information Owners and Information Custodians must also complete a Privacy Impact Assessment before moving the data to the cloud as part of the process of determining the security classification of the data. The context in which the data will be gathered or used in the cloud service will be an important factor in the Privacy Impact Assessment as well.

1.3.2 b) Security of cloud services

Information Owners and Information Custodians must:

- Conduct a Security Threat and Risk Assessment to determine whether the cloud service is appropriate for the information security classification of the data to be transmitted, processed, and/or stored in the cloud based on legal and regulatory risks to government (e.g., copyright, data protection, financial regulation, privacy protection and corporate governance);
- Document, maintain and verify that all information security provisions for the use of cloud services are based on the information security classification of the data that will be transmitted, processed and/or stored in the cloud; and,
- Determine that the cloud vendor can provide the required information security measures that are determined by the information security classification of the data to be transmitted, processed and/or stored in the cloud.

1.3.2 c) Technical specifications

Use of cloud services must not weaken the security of existing systems and infrastructure. Information Owners and Information Custodians must ensure that technical means of protecting information placed in the cloud include:

- A technical security infrastructure that is compatible with the architecture and infrastructure used by the cloud service provider;
- Compatibility of client systems for each cloud service with corporate standards (e.g., by monitoring browser version and plug-in requirements);
- Use of secure communication techniques between government and cloud services (e.g., by deploying VPN, TLS, HTTPS or similar);
- Availability of electronic discovery or equivalent access to search and preserve log data in order to enable and support security investigations, evidence collection and response to legal hold requests; and
- Availability of automated technologies to log, monitor, correlate and alert across the infrastructure that is providing the cloud services to ensure that security breaches and compromises are detected and addressed adequately by the cloud service provider;

Sensitive information stored and processed in the cloud must be protected against co-mingling by separating the organisation’s information from that of other organisations. The use of encryption, obfuscation or tokenization is required when using cloud services to protect the confidentiality and integrity of the information.

Guidelines:

Encryption, tokenization of the data does not always guarantee the confidentiality of the data. Depending on how the various standards are adopted by the cloud vendor, security of the data placed with the cloud vendor is not guaranteed even if the vendor attests to a long list of certifications.

Recommended Tests:

Note: 1.3.2 is reported on the annual information security review.

- Demonstrate that the information to be moved to the cloud has an information security classification.
- Demonstrate a Security Threat and Risk Assessment and Personal Impact Assessment have been completed for the cloud service.
- Demonstrate that the cloud vendor has been assessed against a standard or a set of standards (e.g., ISO 27017, ISO 27018, NIST 800-53, CSA Cloud Control Matrix Level 2, FedRAMP Moderate, Government of Canada PBMM Security Control Profile, etc.)

1.3.3 The use of cloud services must not impede the availability of information and information services.
a) Assurance of information availability

Purpose: To ensure the continued availability of information required to conduct business.

1.3.3 a) Assurance of information availability

Information Owners and Information Custodians must ensure the availability of access to information stored in the cloud by:

- Investing in robust, reliable Internet connectivity;
- Establishing multiple methods of connection (e.g., wired network, wireless and 3G/4G);
- Providing required network bandwidth between the organisation's network and the cloud service provider to avoid poor network latency; and,
- Maintaining links with the legacy systems.

Guidelines:

Poor network connectivity can affect end user experience, availability of cloud services, and if severe enough, can cause data corruption as well. End user experience must be taken into account when designing the infrastructure to connect to the cloud as it impacts cloud adoption.

Recommended Tests:

Note: 1.3.3 is not reported on the annual information security review.