IM/IT Architecture & Standards Manual **STANDARD** **Office of the Chief Information Officer** **Province of British Columbia**	**Effective Date: 2011-01-01** **Scheduled Review: Annual** **Last Updated: 2010-08-27** **Last Reviewed: 2010-08-27**
	Type: Process
6.0 Information and Technology Security (CPPM 12.3.6)	
6.11 Standard for Information Security Threat and Risk Assessment Methodology, Process and Assessment Tool	
Keywords: Risk, Assessment, Risk Assessment, Compliance, Criticality, STRA, iSMART, Security Review, Risk Management, Information Security	

Description of Standard

This Standard supports the efficient, secure operation of information systems while maintaining privacy, and maximizes the effectiveness and efficiency for information technology planning, design, implementation and operations. The Standard focuses on the minimum requirements to complete information Security Threat and Risk Assessment (STRA) and provides an analytical approach to information security risk management.

This Standard defines the methodology, process and tools for performing an information Security Threat and Risk Assessment. The methodology is aligned with the government's Enterprise Risk Management (ERM) Model and provides additional specific details on Information Management/Information Technology (IM/IT) security threats and risks.

As per the government information security policy chapter 2.1.3 b, information ownership flows from the Crown to government Ministers to Deputy Ministers (or equivalent). Information ownership may be further delegated by the Deputy Minister. Information Owners have the responsibility and decision making authority for information throughout its life cycle, including:

- Be involved with security reviews and/or audits;
- Define security requirements during the planning stage of any new or significantly changed Information system; and
- Ensure information and information systems are protected commensurate with their information classification and value.

Information Owners and Information Custodians must conduct an information Security Threat and Risk Assessment to ensure that projects involving information, system development or acquisition activities are completed in accordance with documented requirements, standards, and procedures. This Standard is intended to address these issues and to establish compliance practices that are in line with the IM/IT security governance and policy frameworks. It also includes assessments of legal and regulatory requirements applicable to government.

The Ministry Information Security Officer (MISO) is responsible for assisting business areas in conducting Security Threat and Risk Assessments.

The information Security Threat and Risk Assessment standard used by government is supported through the Information Security Management and Risk Tool (iSMART). The Fundamental Information Risk Management (FIRM) methodology is used herein for managing information risk through a practical and constructive approach of evaluating and driving risk down to acceptable levels. iSMART is used to assist in assessing and measuring the effectiveness of information security management that enables information risk to be managed systematically across the B.C. government

iSMART allows Ministry Information Security Officers (MISOs) and the Office of the Chief Information Officer (OCIO) to identify information security issues, monitor mitigation activities, ensure compliance to standards and policies and report on the governments information security posture.

iSMART enables information security risks to be identified and measured using the Risk Register referred to as the HARM Reference Table. The HARM table is used as an objective basis for assessing the worst-case business impact and the level of harm that has been – or could be – caused by a disruption to or loss of the confidentiality, integrity or availability of business information. It can also be used to provide a common basis for evaluating other risks. See Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary for further detail.

iSMART is also used to assist in mitigating and establishing an information security risk monitoring capability in government. The risk tool serves as a repository for information Security Threat and Risk Assessments and enables authorized personnel to view individual organization results, ministry results and cross-government results.

Minimum information Security Threat and Risk Assessment Standard Requirement:

1. ***All IM/IT projects* must select any one of the Basic of Evaluation (BoE) scorecards listed, and complete the top-level sections (A through I – 61 statements) within the risk tool located in iSMART. (Each response to a question should be substantiated by adding comments, and attaching or providing a reference to the supporting documentation.)***

2. ***Any identified issues, risks and recommendations are to be entered into the issues log and action plan and remediation action provided. (This requirement can be met by attaching or providing a reference to the supporting documentation within the issues log and action plan.)***

iSMART Basis of Evaluation (BoE) Scorecards:

ISO 27001 or
Information Risk Assessment (IRA) or
Standard of Good Practice (SoGP)

It is highly recommended that further analysis of risk and compliance be undertaken by completing the underlying questions associated with the BoE scorecard chosen.

An Information Owner or Custodian may choose to complete a more detailed assessment based on the initial risk review and risk tolerance/acceptance of the ministry. When the initial risk assessment reports a high or medium risk to a system, a more detailed review as described in the Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary is required.

* An Information Management / Information Technology (IM/IT) project is any project or initiative which involves information, information system development or acquisition activities.

Where to Apply This Standard

This Standard is meant for any ministry, public agency or external service provider that is responsible for managing B.C. Government's information. For maximum effectiveness, information Security Threat and Risk Assessments must be completed on every project involving information, a new application, service, system, and/or environment or whenever a major change is proposed.

This Standard is intended to be used government-wide as a guide to understand and generate their project specific information Security Threat and Risk Assessment's using the iSMART tool. It is intended primarily for Information Owners and Information Custodians and those individuals who are responsible for measuring and controlling information risk.

Authority and Exemptions

If there are, compelling business reasons why an organization is unable to comply with this standard, the organization's CIO may authorize a submission for exemption through the OCIO.

Metrics and Enforcement

All required documents in the information Security Threat and Risk Assessment Process Checklist should be completed, reviewed and signed off. See Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary for further detail.

The intention of the OCIO is to advertise and promote this information Security Threat and Risk Assessment standard as being mandatory throughout government. However, in order to effectively manage information security, ministries and other government agencies are expected to adopt and monitor compliance to this Standard. The OCIO Information Security Branch will also monitor for compliance.

When requested, the Office of the Comptroller General's Internal Audit group and the Office of the Auditor General will be provided with high-level or detailed reports. These reports may assist them in determining how Information Security related risks are being addressed within government.

Supporting documentation and supplemental information relating to the information Security Threat and Risk Assessment standard is available on the Information Security Branch website – Compliance web page:

- Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary
    - Information Security Threat and Risk Assessment Process
    - Fundamental Information Risk Management (FIRM) methodology and
    - HARM Reference Table

Terms and Definitions

Any IM/IT device, security and network terminology found in this Standard will be included in a Consolidated Glossary which is under development by the OCIO.

References

Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary
https://gww.cio.gov.bc.ca/services/security/compliance/documents/info_stra_methodology_supplementary.pdf

Information Security Management and Risk Tool (iSMART)
https://gww.iscm.cio.gov.bc.ca

Core Policy and Procedure Manual (CPPM) Chapter 12
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm

Information Security Policy
http://www.cio.gov.bc.ca/cio/informationsecurity/policy/securityinformationpolicy.page

IM/IT Standards Manual
http://www.cio.gov.bc.ca/cio/standards/standards_manual.page

Enterprise Risk Management
http://www.fin.gov.bc.ca/PT/rmb/index.shtml

All policy references that support this information security threat and risk assessment standard are located in Appendix II of the Security Review: Information Security Threat and Risk Assessment Methodology and Process Supplementary.

Additional Information

Compliance Management, Information Security Branch, OCIO, is the owner of this standard. Its website is located at https://gww.cio.gov.bc.ca/services/security/compliance

Contact

Information Security Branch, OCIO
Email: CITZCIOSecurity@gov.bc.ca