BRITISH COLUMBIA | Ministry of Citizens' Services

Security Threat and Risk Assessment Standard

Information Security Branch
Office of the CIO, Province of BC

Document Version: 3.0
Replaces Version: 2.0
Published: ***June 2020***

I Document Revision History

Revision Date	Author	Document Version	Change Reference
November 2019	Brian Horncastle	v3.0	Material and whole re-write of standard

II Standard Introduction

Purpose: The purpose of this standard is to set requirements for efficiently assessing (identifying, analyzing, and evaluating), defining planned treatments, and reporting security threats and risks in information systems. This standard identifies the components of a Security Threat and Risk Assessment (STRA) and expectations related to their completion. STRAs are important for the overall protection of information systems and to ensure reasonable security. This principle-based standard is intended to support and enable a modern digital government by allowing for modality and flexibility and is designed to be usable in the field. The STRA Guidelines document provides terms and definitions, clarifies approach, and provides an explanation of the Statement of Acceptable Risks (SoAR) which is used to complete a Security Threat and Risk Assessment.

Description: This standard applies to all government organizations (ministries, public agencies, boards, and commissions), service providers, and any other entity managing the Government of British Columbia's information which is subject to Information Security Policy, Information Security Standard, Information Security Classification Standard, Core Policy & Procedures Manual, and legislation.

III Terms and definitions

Terms and definitions are covered in the Security Threat and Risk Assessment Standard Guidelines document.

1 Security Threat and Risk Assessment Standard

1.1 An STRA must be conducted for all information systems during planning, development and implementation. A review and updated STRA must be conducted throughout the life of an existing information system for any significant or material change(s) and must also consider any previously identified risks. The head of the government organization is accountable for ensuring that appropriate and reasonable support and resources are provided for this to occur.

1.2 A review schedule must be maintained to ensure that STRAs are periodically conducted throughout the life of an information system.

1.3 Service delivery units must engage, communicate, and consult with their respective Ministry Information Security Officer when an STRA is required.

1.4 Within their portfolio, Ministry Information Security Officers are responsible for assisting service delivery units in conducting STRAs and engaging related system stakeholders.

1.5 OCIO's Information Security Branch is responsible for the ongoing development, maintenance, continuous review, improvement, and support of this standard.

1.6 OCIO's Information Security Branch is responsible for monitoring of compliance to this standard.

1.7 OCIO's Information Security Branch shall provide STRA related templates, guidelines, process and procedure documentation, and training to MISOs where appropriate.

1.8 STRAs should be conducted by resources with appropriate expertise and experience with information security and the related technologies used by the system being assessed.

1.9 The criticality of an information system and security classification of information stored and handled by the system should be reviewed and considered when conducting an STRA as this information is helpful to accurately and reasonably assess security risk and to establish the context for the STRA.

1.10 A lite or comprehensive STRA may be used depending on the appropriateness commensurate to the information system being assessed with consideration to the achievement of reasonable security. A lite STRA can be achieved through completion of a SoAR on its own. A comprehensive STRA can be achieved through completion of supporting documentation, evidence collection where available, and a SoAR.

1.11 Ministry Information Security Officers may use their best judgement and discretion in how supporting documentation and evidence collection for an STRA is approached and are encouraged to follow industry best practices.

1.12 To determine the reasonableness of a system's security, each risk assessed must consider the likelihood to which a threat may leverage a weakness, the potential impact, and an acknowledgement of what this could mean to the organization.

1.13 Information security risks may be determined using a control driven, threat modeling or hybrid approach.

1.14 The scope of potential impact must be documented (e.g. impact to business unit, ministry only, parts of government or all of government, citizens, or other stakeholders).

1.15 For each risk that is identified, a planned treatment or acceptance must be documented.

1.16 Risk findings from the STRA activity must be recorded via an OCIO-approved SoAR tool.

1.17 At minimum, a SoAR must be reviewed and signed at an appropriate level as defined within an OCIO approved SoAR tool. All completed and signed SoARs must be submitted to the OCIO's Information Security Branch. This constitutes the closure of an STRA.

1.18 Ministries will not accept risks which are likely to have a corporate or government-wide impact. Such risks shall be documented with a note indicating that the risk is corporate in nature and will be communicated to OCIO via a SoAR.

1.19 Risks which require treatment after the completion of a SoAR must be tracked in a risk register.

2 Authority

- Information Security Policy
- Information Security Standard
- Information Security Classification Standard
- Core Policy & Procedures Manual

3 Supporting Documents

- Security Threat and Risk Assessment Guidelines
- Statement of Acceptable Risks

4 Contact

- Ministry Information Security Officers