1. 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.

2. DESCRIPTION

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 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 **6.11 Security Threat Risk Assessment Standard (STRA) Specifications** document provides terms and definitions, clarifies approach, and explains the Statement of Acceptable Risks (SoAR) which is used to complete a STRA.

In addition to this standard, the **6.11 STRA Specifications** document provides detailed requirements. The specifications outlined in the **6.11 STRA Specifications** document MUST be followed in conjunction with this standard.

3. AUTHORITY

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

4. APPLICATION / SCOPE

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 Core Policy & Procedures Manual, Information Security Policy and Information Security Standard. This standard MUST be read in conjunction with the **6.11 STRA Specifications** document that provides mandatory specifications for the requirements in Section 5.

5. REQUIREMENTS

a) A STRA MUST be conducted for all new information systems and be kept updated throughout an information system's lifecycle. See **6.11 STRA Specifications** **Section 5** for more details.

b) The STRA for an existing information system MUST be reviewed and updated whenever there are any significant or material change(s) and:

- Previously identified risks reassessed and updated; and,
- New risks that are identified, documented.

c) A review schedule MUST be maintained to ensure that STRAs are reviewed and re-evaluated throughout the life of an information system. The frequency of the STRA review MUST be based on maintaining the target risk level for the information system.

d) When a STRA is conducted, it MUST be based on the criticality of the information system and the information security classification of information stored and handled by the system.

e) Service delivery units MUST engage, communicate, and consult with their respective Ministry Information Security Officer when an STRA is required. See **6.11 STRA Specifications** **Section 5** for more details.

f) 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).

g) Information security risks MUST be assessed based on:

- How likely a threat will leverage an exposed security weakness (a.k.a vulnerability) or gap; and,
- The potential impact to the organization if the risk is realized. See **6.11 STRA Specifications** **Section 5** for more details.

h) Risk findings from the STRA activity MUST be recorded via an OCIO-approved tool[1]. See **6.11 STRA Specifications** **Section 5** for more details.

i) For each risk that is identified, a planned treatment or acceptance MUST be documented.

j) Risks which require treatment after the completion of the risk assessment MUST be tracked in a risk register and managed.

k) Ministries MUST not accept risks which are likely to have a corporate or government-wide impact. Such risks MUST be documented with a note indicating that the risk is corporate in nature and will be communicated to OCIO via the approved tool[1].

l) At minimum, a STRA activity MUST result in a Statement of Acceptable Risks (SoAR) artifact that has been reviewed and signed by an accountable individual. See **6.11 STRA Specifications** **Section 5** for more details.

m) All completed and signed SoARs MUST be submitted to the OCIO's Information Security Branch. This constitutes the closure of an STRA.

6. DEFINITIONS/GLOSSARY

Refer to the **6.11 STRA Specifications** **Section 6** for more information.

[1] Contact VulnerabilityandRiskManagement@gov.bc.ca for more information on the approved tool.

7. SUPPORTING DOCUMENTS

- 6.11 Security Threat Risk Assessment Specifications.

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revisions
V3.0	November 2019	Brian Horncastle	Material and whole re-write of standard.
V3.1	September 2022	Sharina Gopaldas Johnston	Document format/layout update to new template.

9. CONTACTS

For questions or comments regarding this standard, please contact:

Information Security Branch, OCIO
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca