6.11 SECURITY THREAT RISK ASSESSMENT SPECIFICATIONS

Abstract

Supporting document for the 6.11 Security Threat Risk Assessment Security Standard. It provides clarification and additional requirements of the standard. It also provides guidance on completing the Statement of Acceptable Risks.

Information Security Branch

infosecadvisoryservices@gov.bc.ca

6.11 Security Threat Risk Assessment Specifications

Document Version: 2.0
Effective Date: November 2019
Last Reviewed: September 2022

Contents

1. INTRODUCTION

This specifications document was developed to provide detailed security requirements to support the 6.11 Security Threat and Risk Assessment (STRA) Standard. The specifications outlined in this document MUST be followed in conjunction with the 6.11 STRA Standard.

The purpose of the Specifications document is to assign responsibilities for this standard, define terms and definitions, clarify approach, and provide linkage to the Defensible Security Framework and an explanation of the Statement of Acceptable Risks (SoAR) which summarizes a completed STRA.

2. DEFENSIBLE SECURITY LINKAGE

The 6.11 STRA Specifications establishes the minimum requirements to establish adequate information security in accordance to government's Defensible Security Framework for the protection of government information assets and government information systems.

The Defensible Security elements that apply to all IM/IT security standards are highlighted in blue in the table below: Executive Support, Roles & Responsibilities, Incident Management, Policy (Information Security), Awareness Program/Courses, and Security Governance.

Additional elements specific to the 6.11 STRA Specifications are highlighted in yellow: Risk Appetite & Register, Risk Assessment, Security Assessment and Information Security Program.

Prerequisites	Directives	Respiration	DNA (Culture)
Executive Support	**Asset** Management	**Backup** & Retention	**Program** (Information Security)
Roles & Responsibilities	**Change** Management	**Logging** & Monitoring	**InfoSec** Classification
Crown Jewels	**Incident** Management	**Physical** & Visible ID	**Aware** Program/Courses
Risk Appetite & Register	**BCP**	**Logical** Access	**Security** Governance
Risk Assessment	**DRP**	**Personnel** Security	
Security Assessment	**Incident** Response	**Defense**-in-Depth (endpoints & networks)	

Prerequisites	Directives	Respiration	DNA (Culture)
	Policy (Information Security)	**VM** & Patching	
	Vendor Requirements	**AppSec**	

3. ROLES & RESPONSIBILITIES

This section lists the general accountabilities and responsibilities for the specific requirements of the standard.

References to the "Owner" in this document shall be considered the same as "System Owner" or "Application Owner" (and in the SoAR document). The Owner is the head of the organization that will use and/or operate the information system being assessed. For example, this can be an Executive Director, Director, Manager, Supervisor, Contractor or Vendor.

If the Owner also owns the information that will be collected, processed, hosted or transmitted by the information system or application, this person assumes the **Information Owner**[1] role and is accountable for:

- Addressing the information security risks identified during the STRA process and documented in a completed SoAR; and,
- Ensuring the resources with appropriate expertise and experience with the line of business/service delivery unit and the related technologies comprising the system being assessed are provided to assist with the STRA activity.

The Owner who does not own the information that will be collected, processed, hosted or transmitted by the information system assumes the **Information Custodian**[1] role. As an Information Custodian, the Owner may be delegated the responsibilities associated with the accountabilities of the Information Owner. Those responsibilities are:

- Conducting a STRA and completing the SoAR for the information system; and,
- Documenting the security risks identified during the STRA in the SoAR.

A Ministry Information Security Officer (MISO) is accountable for:

- The ministry risk register; and,
- Identifying corporate risks.

[1] See Security Roles and Responsibilities for more information on this role.

The responsibilities associated with the above accountabilities are:

- Assisting service delivery units within their portfolio to conduct STRAs, i.e. completing SoARs;
- Engaging with stakeholders related to system being assessed;
- Ensuring the criticality of an information system and security classification of information handled by the system is reviewed and considered when the STRA is conducted;
- Using their best judgement and discretion in how supporting documentation and evidence collection for a STRA is approached;
- Updating the ministry risk register with the risks from the SoAR; and,
- Notifying the OCIO's Information Security Branch of the corporate risks.

The Chief Information Security Officer (CISO) is accountable for the following responsibilities that are delegated to the OCIO's Information Security Branch:

- Ongoing development, maintenance, continuous review, improvement, and support of the STRA Standard;
- Monitoring the compliance of government organizations to the STRA standard; and,
- Provision of STRA related tools, templates, specifications, guidelines, process, documentation, and training to MISOs.

4. RESPONSIBILITY ASSIGNMENT MATRIX (RACI CHART)

This section summarizes the deliverables of this standard.

RACI: **R** = Responsible; **A** = Accountable; **C** = Consult; **I** = Inform

Security Threat Risk Assessment (STRA) Standard Deliverables	**Roles**									
	Information Owner[2]	**Information Custodian**[3]	**Government Chief Information Officer (GCIO)**	**Ministry Chief Information Officer (MCIO)**	**Chief Information Security Officer (CISO)**	**Ministry Information Security Officer (MISO)**	**Executive Director/ Director/ Manager/ Supervisor**	**Employee**	**Contractor**	**Vendor**
A completed SoAR for each information system. [4]	**A**	**R**		**I**	**I**	**CR**	**R**		**R**	**R**
A risk register documenting the residual risks identified in the SoAR. [5]	**CR**	**CR**	**I**	**I**	**C**	**AR**	**CR**		**CR**	**CR**

[2] In accordance to Security Roles and Responsibilities, an Information Owner has the accountability and responsibility for the security and management of government information for its entire lifecycle, but not necessarily the information system itself. The Information Owner can delegate the responsibility for the security and management of government information to an Executive Director, Director, Manager, Supervisor, Contractor, or Vendor.

[3] An Executive Director, Director, Manager or Supervisor of a Service Delivery Unit, or a Contractor or Vendor who has been delegated the responsibility for the security and management of an information system is deemed an Information Custodian.

[4] The Information Owner is accountable for ensuring a SoAR is completed for the information system. Information Custodian is responsible for completing a SoAR while the MISO provides consultation. The MISO is then responsible for submitting the completed SoAR to the OCIO.

[5] The MISO is both accountable and responsible for maintaining the risk register. The Information Owner, Information Custodian, Executive Director/Director/Manager/Supervisor, Contractor and/or Vendor are consulted and are responsible for identifying the risks to the MISO.

Security Threat Risk Assessment (STRA) Standard Deliverables	**Roles**									
	Information Owner[2]	**Information Custodian**[3]	**Government Chief Information Officer (GCIO)**	**Ministry Chief Information Officer (MCIO)**	**Chief Information Security Officer (CISO)**	**Ministry Information Security Officer (MISO)**	**Executive Director/ Director/ Manager/ Supervisor**	**Employee**	**Contractor**	**Vendor**
Documented treatment plan or acceptance and impact for each risk identified in the SoAR.	**A**	**R**		**I**	**I**	**C**	**R**		**R**	**R**
Documented and identified corporate risks.[6]	**I**	**I**	**I**	**I**	**I**	**AR**	**I**		**I**	**I**
STRA related tools, templates, specifications and guidelines.					**AR**[7]	**I**	**I**		**I**	**I**

[6] The MISO is both accountable and responsible for identifying corporate risks.

[7] The person in the CISO role is accountable and the CISO's office is responsible for developing and publishing the STRA related tools, templates, specifications, and guidelines.

5. SPECIFICATIONS

a) A STRA is the overall activity used by the BC public service to assess and report security risks for an information system and the information it stores, processes or transmits. It is a key enabler for responsible and secure digital delivery of government services.

b) STRAs ensure there is reasonable security protections in place for the information system and information assets being assessed.

c) The goal of a STRA is to produce a SoAR. The SoAR documents all risks identified as related to the information system, their rating, and recommended treatment plans. The identified risks in the SoAR MUST be recorded in an OCIO-approved[8] tool.

d) The rating of an information security risk MUST be based on how likely a threat that will leverage an identified exposed security weakness or gap, and the potential impact from the realized risk to the organization.

e) STRAs are key to empowering the management of government organizations to make informed risk-based decisions about the information systems and information assets they are accountable and responsible for. SoARs provide snapshots in time of STRAs that raise the awareness of system security risks in an organization. SoARs MUST be completed prior to implementation of a new system or significant/material changes to an existing system.

5.1. APPROACH

Modality is the ability for a Security Threat and Risk Assessment to be conducted in more than one defined manner. Modality gives flexibility to Ministry Information Security Officers to document risks relative to the importance of the information system being assessed. This is intended to allow for the overall activity to occur at the fastest pace possible, with the lowest potential cost, and with the greatest equity while still adequately assessing and documenting security risk. Allowing for modality helps to enable an approach consistent with the principles of a digital government.

a) The decision on the type of STRA to be conducted on an information system being assessed to ensure reasonable security MUST be commensurate with:
   i. The criticality of the information system; and,
   ii. The information security classification of the information that will be handled by the information system.

b) The MISO should work with the owner of the system to decide whether to conduct a lite STRA or a comprehensive STRA as follows:

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

i. If the system being assessed is critical or handles confidential information, then a comprehensive STRA approach is required. A comprehensive STRA consists of supporting documentation, evidence collection where available, and completion of SoAR.

ii. If the system being assessed is not critical and does not handle confidential information, then a lite STRA approach could be considered. In cases where additional evidence and supporting documentation is not required, a lite STRA can be achieved through completing a SoAR on its own.

c) When conducting a STRA, a MISO may choose to use a:

- Threat modeling approach;
- Control driven approach; or,
- A hybrid of the above two approaches.

5.1.1. Threat Modelling Approach

a) A threat modeling approach determines risks by:

- Identifying assets;
- Describing their architecture;
- Decomposing the application or system;
- Identifying and documenting threats;
- Rating the threats; and then,
- Using the threats as the basis for the remainder of the risk assessment.

b) If a threat modeling approach is used, it is recommended to leverage an industry recognized threat modeling methodology.

5.1.2. Control Driven Approach

a) In the context of a STRA, a control driven approach leverages a pre-defined list of controls, i.e. a control set, as a guide to check for the existence of related risks for the system being assessed. This assessment should not be compliance focused as it does not assure reasonable security for the system.

b) If a control driven approach is used, it is recommended to leverage a relevant industry recognized control set.

5.2. RISK TREATMENT

a) A treatment plan MUST be documented for each risk to identify what you plan to do about the risk. Documenting risk treatments are within the scope of a STRA.

b) Risk treatments should occur, but their occurrence is not a condition for the completion of a STRA. The execution of risk treatments is outside the scope of a STRA activity.

c) Planned risk treatments are documented at a high-level in the SoAR. Valid risk treatments are:

   i. Accepting the risk as is;
   ii. Remediate (fix);
   iii. Mitigate (reduce);
   iv. Transfer (insure); or,
   v. Avoid (make a change so the risk no longer applies).

5.3. STRA REVIEW

Over time, the accumulation of minor changes to an information system can represent a significant or material change. These collective changes can result in new unidentified security risks. Even if no changes are made to the information system, new vulnerabilities that are discovered over time can cause the security state of a system to degenerate.

a) Service Delivery Units and MISOs MUST plan review schedules to update information system STRAs to pre-emptively identify security risk changes since the last assessment and follow-up on them. This avoids assumptions regarding the security state of the information system.

b) STRAs should be reviewed as follows:

   i. For critical systems, annually at minimum.
   ii. For non-critical systems, once every 2 years at minimum.

5.4. STATEMENT of ACCEPTABLE RISKS

a) At minimum, a SoAR MUST be signed off by the appropriate parties (see Section 5.4.3) to be considered completed. This is to ensure that the risk assessment information was reviewed and accepted by the MCIO.

b) Completed SoARs MUST be submitted to the Chief Information Security Officer (CISO). The Information Security Branch of the OCIO will store the submitted SoARs in a central repository to enable tracking, follow-up, and analytics. This is to inform strategic corporate information security and risk management activities and initiatives.

5.4.1. Section A: TRACKING INFORMATION

This section provides information needed for tracking and follow-up. The following table describes the fields in this section:

Field name	Description
Assessment Reference Number	This is a unique reference number created by the Primary Risk Evaluator. It is assigned to a STRA by the ministry. This number is documented in the Statement of Acceptable Risk (SoAR) and any supporting STRA documentation.
System Name	A short name that accurately describes the system that is the subject of the assessment.
Division	The Division that is responsible for the system.
Ministry	The Ministry that owns the system.
System stores or handles confidential information	If the system stores or handles confidential information, the answer is yes. Note, the level of due diligence applied in the STRA MUST be commensurate with the information security classification label, i.e. Public, Protected A, Protected B, or Protected C. See the IMIT 6.18 Information Security Classification Standard for a description of classification levels.
Critical System	Check this box if a system has been classified as critical. If the system is classified as critical, the assessment of critical systems MUST be performed in compliance with the IMIT 5.10 Critical Systems Standard.
Type	Select 'LITE' if a decision was made to complete the SoAR only. This applies only if the system is not critical and does not contain confidential or personal information. Select 'COMPREHENSIVE' if the system is critical or contains confidential or personal information. Select this option as well if the MISO decides that an in-depth STRA is more appropriate.
Primary Risk Evaluator	Name of the person who has gathered the information, analyzed, and documented the risks related to the system being assessed. Usually this is the MISO.
Owner	The Name of the head of the division or ministry accountable for the delivery or operations of the system that is the subject of the SoAR.

Field name	Description
SoAR is Confidential/ Shareable/ Indexable in STRA INVENTORY	The OCIO maintains a central inventory of all government SoARs, i.e. the STRA Inventory site[9]. This inventory helps ministries determine whether a STRA has already been completed for a system. Select one of the options from the drop-down list: • Is Shareable • Is Confidential • Is Indexable, but not shareable Only MISOs and other approved users can search the inventory. The “Is Shareable” option informs the OCIO to list your SoAR in the inventory and to share it. The sharing of SoARs increases transparency and reduces redundancy, re-work, and time for others across government who are completing an assessment for the same system. Documented risks for the system may also be applicable to the assessment that another MISO is working on. The “Is Confidential” option informs the OCIO to not list your SoAR in the inventory. Typically, you would check this box if the knowledge of the SoAR itself could cause harm and must be kept confidential. The “Is Indexable, but not shareable” option informs the OCIO to only list your SoAR in the inventory. Only the document title and relevant meta-data will be accessible. The rest of the SoAR content will be inaccessible to the other MISOs and approved users.
Scope	Choose which level the STRA was conducted at, i.e. ministry or corporate level.
Cloud Service Type	Select one of the options provided: • Not cloud – Choose this option if the application or system that is being assessed is hosted in a government data centre or on a local machine;

[9] Please email VulnerabilityandRiskManagement@gov.bc.ca for access to the STRA Inventory site.

Field name	Description
	• IaaS – Choose this option if the system is Infrastructure-as-a-Service (IaaS) based. For IaaS-based systems, the Cloud Service Provider (CSP) provides virtualized infrastructure resources such as servers, storage and network are provisioned and managed over a wide area network (WAN) to the consumer. The consumer does not manage or control the underlying cloud infrastructure but has control over their provisioned resources where they are able to deploy and run software, which can include operating systems and applications. Applications, networks, and firewall configurations are typically included are the responsibility of the consumer, e.g. setting up of the firewalls for Amazon; • PaaS – Choose this option if the system is Platform-as-a-Service based. For PaaS-based systems, the CSP manages the infrastructure (as in IaaS) and also the operating system, middleware and runtime. The CSP provides PaaS products that are-designed for consumers i.e. developers, that enables them to develop, run and manage their applications without having to build and maintain the infrastructure and platform. Data and the user access/identity management and applications scope are the responsibility of the consumer; • SaaS – Choose this option if the system is a Software-as-a-Service based solution. SaaS-based systems are licensed on a subscription basis (or free) and typically require no installation and minimal management. As recommended in the Hosting and Application Development Strategy, adoption of a SaaS product must fully respect the SaaS delivery model. With this model, the vendor/Cloud Service Provider is responsible for application patches and upgrades and must be able to implement these on their schedule without impacting users of the application. Data and

Field name	Description
	the user access/identity management are the responsibility of the consumer; • Serverless - Also known as Abstracted Services. Involves no server management for consumer/end user. Usually automatic scaling and availability are part of this. Typically, event driven functions would be included. Data and the user access/identity management are the responsibility of the consumer. For example, an application is deployed by the user, but the backend infrastructure (setup, patching, maintenance, scalability, etc.) is abstracted from the user and happens behind the scenes transparently; • Other – Choose this option if the system is not one of the above-mentioned categories.
Short Description	Provide a concise description that explains what the SoAR is about i.e.: • purpose of the system and what it does; • high-level findings of the assessment on the system; and, • recommendations from the assessment. If no risks will be documented in Section B: Risk Assessment Table, explain why here.

5.4.2. Section B: RISK ASSESSMENT TABLE

a) 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.

b) This section documents the risks that were identified during the assessment. If no risks are documented here, provide a reference to the location of the related risk documentation.

Instruction: If more rows are needed, copy and paste from an existing row to keep the built-in dropdowns.

Field name	Description
Risk Ref #	This is a unique reference number for the risk identified in the STRA within the STRA and SoAR.
Risk Name	This should be in a few short words to portray the gist of the risk to the reader.
Primary Risk Type	This field is intended to help the reader to understand the nature of the identified risk. Categorize the risk by selecting one of the options from the drop-down list or clear the field and enter in your own response manually: • Access • Availability • Brute force • Compliance/regulatory/legal • Compromised critical hosts • Confidentiality • Credential theft • Cyber incident • Distributed/Denial of service • Domain-based • Exploit/exploit of vulnerability • Financial • Hacking • Hacktivism • Health and safety/physical threat • Identity • Insider • Integrity • Malware • Man-in-the-middle

Field name	Description
	• Mobile • Operational • Phishing/social engineering/fraud • Physical infrastructure/office building/data centre • Ransomware/extortion • Reputational • Spam • Spoofing • Website defacement • OTHER (Please enter other risk type)
Risk Rating	This field is intended to provide the reader an understanding of how serious the risk is. Select one of the following risk ratings from the drop-down list: • Very Low • Low • Medium • High • Critical
Treatment Plan	This field is not intended to be detailed. It is intended to provide a very high-level course of action for the risk. Select one of the options from the drop-down list: • Plan – Accept risk as is • Plan – Treat: Remediate (fix) risk • Plan – Treat: Mitigate (reduce) risk • Plan – Treat: Transfer risk (e.g. insurance) • Plan – Treat: Avoid (make a change so the risk no longer applies) • Plan – None
Short Description	This field is intended to assist the reader to better understand the risk and or treatment. The primary risk evaluator should provide information that would assist in that. The description should be as concise as possible.

5.4.3. Section C: ACCEPTANCE

This section documents the approvals for the SoAR. Additional signature blocks may be added to address the ministry's needs.

a) The Owner, MISO, and the person accountable for the system, i.e. Deputy Minister (DM), Ministry Chief Information Officer (MCIO) or delegate, MUST sign and date the SoAR to complete it. A delegate is the person authorized by the DM or MCIO to sign the SoAR on their behalf. The delegate MUST ensure that the DM is made aware of the information security risks. This is to ensure the DM can fulfill the duties related to making reasonable security arrangements for the protection of information.

b) The completion of a SoAR marks the completion of a STRA. Send the completed SoAR to the Chief Information Security Officer (CISO) via the OCIO approved tool. The CISO will sign it as an acknowledgement of receipt. The CISO's signature on the SoAR document does not mean acceptance of the risks documented in SoAR.

6. DEFINITIONS/GLOSSARY

See Information Security Glossary. Terms used exclusively in the 6.11 STRA Specifications are listed in the table below.

Term	Definition
Critical System	See IMIT 5.10 Critical Systems Standard.
Government organizations	Within the context of a STRA, government organizations are defined as ministries, public agencies, boards, and commissions which manage the Government of British Columbia's information and are subject to Information Security Policy, Information Security Standard, Information Security Classification Standard, Core Policy & Procedures Manual, and legislation.
Head of a government organization	For a ministry or public agency, the head of the organization is typically a deputy minister. For a board, the head of the organization is normally the chair. For a commission, the title referring to the head of the organization may vary.
Information System	Within the context of a STRA, this can be any of the following that could introduce information security risk to government: • A collection of manual and automated components that manages a specific data set or information resource as defined in Core Policy & Procedures Manual Chapter 12. • It is a system (including people, machines, methods of organization, and procedures) which provides input, storage, processing, communications, output and control functions in relation to information and data. • Computerized systems, including data processing facilities, data base administration, hardware and software which contain machine-readable records.

Term	Definition
Material change	Within the context of a STRA, a "material change" is any change to an information system which could affect an important element of its security.
Portfolio	All parts of the organization for which an employee is responsible for providing a service to.
Risk	Within the context of a STRA, it is an acknowledgment of how likely a threat is to leverage a vulnerability, what the potential impacts could be, and what it means to the organization.
Service Delivery Unit	Any unit within an organization which is tasked with the responsibility to deliver a service.
Significant change	Within the context of a STRA a "significant change" is any major change to an information system.

7. SUPPORTING DOCUMENTS

- IMIT 6.18 Information Security Classification Standard
- Understanding the reference STRA process section
- Statement of Acceptable Risks template
- Security Threat and Risk Assessment Approaches – Informational Paper[10]
- Defensible Security Framework
- Security Roles and Responsibilities

8. REVISION HISTORY

Version	Revision Date	Author	Description of Revisions
V1.0	November 2019	Brian Horncastle	New guidelines document to support the Security Threat and Risk Assessment Standard v3.0
V1.1	June 2021	Ryan Bluemel	Updates to definitions.
V2.0	September 2022	Sharina Gopaldas Johnston	New information added and document format/layout update to new template. Guideline document renamed to Specifications document.

[10] Email VulnerabilityandRiskManagement@gov.bc.ca to request this document.

9. CONTACTS

For questions or comments regarding this standard, please contact:
Information Security Branch, OCIO
Ministry of Citizens' Services
Email: InfoSecAdvisoryServices@gov.bc.ca