BRITISH COLUMBIA | Ministry of Citizens' Services

Security Threat and Risk Assessment Standard Guidelines

Information Security Branch
Office of the CIO, Province of BC

Document Version: 1.1

Published: ***January 2020***

I Document Revision History

Revision Date	Author	Document Version	Change Reference
November 2019	Brian Horncastle	V1.0	New guidelines document to support the Security Threat and Risk Assessment Standard v3.0
June 2021	Ryan Bluemel	V1.1	Updates to definitions.

II Guidelines Introduction

Purpose: The purpose of this guidelines document is to define terms and definitions, clarify approach, and provide an explanation of the Statement of Acceptable Risks (SoAR) which is used to complete a Security Threat and Risk Assessment.

Description: This guidelines document applies to the Security Threat and Risk Assessment Standard.

III Terms and definitions used in the standard

Term	Definition
Comprehensive STRA	A comprehensive STRA consists of supporting documentation, evidence collection where available, and completion of a Statement of Acceptable Risks (SoAR). This or a lite STRA can be conducted commensurate to the information system being assessed with consideration to the achievement of reasonable security. A comprehensive STRA may be used for example when assessing risk for critical systems and systems which store or handle confidential information.
Control driven approach	A control driven approach can be used to identify risks by leveraging a pre-defined list of controls and using those as a guide to check for the existence of related risks. In the context of a Security Threat and Risk Assessment, the use of controls is for the purpose of determining risks VS being a compliance-focused exercise. An alternate approach to control driven is threat modeling, or hybrid.
Critical System	See Critical Systems Standard.
Digital Government	Digital governments use the culture, processes, business models and technologies of the internet era to improve the way they work. As a government, this means being able to work across organizational boundaries (inside and outside government) to share tools, data and learning to deliver government's priorities at the fastest pace, lowest cost and greatest equity. Becoming a digital government means using digital tools and approaches to provide easy to use online services for all British Columbians and to use trusted information to understand and address today's complex social challenges.
Government organizations	Within the context of the Security Threat and Risk Assessment Standard 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.
Hybrid approach	In the context of control driven and threat modeling approaches to STRAs, a hybrid approach is a combination of those two approaches.
IM/IT	Information Management / Information Technology
Information System	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. Normally used to describe computerized systems, including data processing facilities, data base administration, hardware and software which contain machine-readable records. A collection of manual and automated components that manages a

	specific data set or information resource. (As defined in CPPM Chapter 12: IM/IT). In the context of a Security Threat and Risk Assessment this is any such thing which could introduce information security risk to government.
Lite STRA	A lite STRA consists of a Statement of Acceptable Risks (SoAR) on its own. This or a comprehensive STRA can be conducted commensurate to the information system being assessed with consideration to the achievement of reasonable security. A lite STRA may be used for example when a system is not critical systems and systems where the system does not store or handle very confidential information.
Material change	Within the context of a Security Threat and Risk Assessment, a "material change" is any change to an information system which could affect an important element of its security.
Ministry Information Security Officer	See definition in Information Security Policy.
Modality	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.
Portfolio	All parts of the organization for which an employee is responsible for providing a service to.
Risk	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.
Security Threat and Risk Assessment	This is the overall activity of assessing and reporting security risks for an information system. STRAs are a type of assessment used by the BC public service to assess digital risks. This is a key supporting enabler for responsible digital government. STRAs are a snap-shot in time and raise the awareness of system security risks in an organization to a level at which risk-based decisions can occur effectively. STRAs are key to empowering management to make informed risk-based decisions about information assets that are directly or indirectly under their control as part of their responsibilities and accountabilities. An STRA also documents risk ratings and planned treatments.
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 Security Threat and Risk Assessment a "significant change" is any major change to an information system.
Statement of Acceptable Risks	The primary goal of a Security Threat and Risk Assessment is to produce a Statement of Acceptable Risks (SoAR) which documents all risks identified as related to the information system, their rating, and

	recommended treatment plan. By requiring sign-off, the SoAR ensures that risk assessment information recommended by Ministry Information Security Officers is reviewed and accepted by the accountable person in the government organization (i.e. normally the Ministry Chief Information Officers) and is then submitted to the Chief Information Security Officer. Each Security Threat and Risk Assessment activity needs to result in a SoAR. The OCIO Information Security Branch will store SoAR's in a central repository for the purpose of providing tracking, follow-up, analytics, and to inform strategic corporate information security and risk management activities and initiatives.
SoAR	Statement of Acceptable Risks.
STRA	STRA stands for "Security Threat and Risk Assessment".
STRA review schedule	The accumulation of minor changes over time, when looked at together, can represent a significant or material change. Planned review schedules to perform updates to information system STRAs is important in helping to ensure security risks are identified and followed-up on. Even if a change has not intentionally occurred, the security state of a system can change over time as new vulnerabilities are discovered. Reviews can help to find risks which have emerged since the last risk assessment and this helps to avoid assumptions regarding security state. Service delivery units and Ministry Information Security Officers are more likely to pre-emptively address security issues when STRA review schedules are in-place and being leveraged.
Threat modeling approach	A threat modeling approach determines risks by first identifying assets, describing their architecture, decomposing the application or system, identifying and documenting threats, rating the threats, and then using this as the basis for the remainder of the risk assessment. An alternate approach to threat modeling is a control driven approach, or hybrid.
Treatment	A treatment plan is documented for each risk to identify what you plan to do about the risk. Documenting the treatments which are planned is within scope of an STRA. Performing the actual treatments should occur but is outside the scope of a Security Threat and Risk Assessment activity and is not a condition for the completion of an STRA. Examples of valid treatments include: accepting risk as is, remediate (fix), mitigate (reduce), transfer (insure), or avoid (make a change so the risk no longer applied). Planned treatments are documented at a high-level in the SoAR.
Cloud Service Type - IaaS	Infrastructure as a Service: 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. Setup the firewalls for Amazon.

Cloud Service Type - PaaS	Platform as a Service: the service provider manages the infrastructure (as in IaaS) and also the operating system, middleware and runtime. PaaS products are designed for developers, enabling 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.
Cloud Service Type - SaaS	Software as a Service: software licensed on a subscription basis (or free), typically requires 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, whereby 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 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. E.g. 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.

1 STRA Approach

- The overall activity of assessing security risks for an information system at a point in time is called a Security Threat and Risk Assessment (STRA).
- At the time an STRA is to be conducted the Ministry Information Security Officer working with the service delivery unit needs to decide to conduct a lite or a comprehensive STRA. This should be commensurate to the information system being assessed and support the achievement of reasonable security.
  - If the system being assessed is critical and if it handles confidential information then it is recommended to consider a comprehensive STRA approach.
  - If the system being assessed is not critical and if it does not handle confidential information, then it is recommended to consider a lite STRA approach. A lite STRA is also appropriate in cases where additional evidence and supporting documentation is not required.
- A Ministry Information Security Officer may choose to use a threat modeling, control driven, or hybrid approach at their discretion.
  - If a threat modeling approach is used it is recommended to leverage an industry recognized threat modeling methodology.
  - If a control driven approach is used it is recommended to leverage an industry recognized control set.

2 Statement of Acceptable Risks (SoAR)

SECTION A – TRACKING INFORMATION

Purpose of section:

This section provides information needed for tracking and follow-up.

Description of fields:

Assessment Reference Number – This is a unique reference number assigned by the ministry which the Primary Risk Evaluator creates and uses for a Security Threat and Risk Assessment (STRA). This reference number should be documented in the Statement of Acceptable Risk (SoAR) and in any supporting STRA documentation.

System Name – A short name that accurately describes the system that is the subject of the assessment.

Division – The Division of the System Owner.

Ministry – The Ministry of the System Owner.

System stores or handles confidential information □ – An acknowledgement of whether the system stores or handles confidential information. If the answer is yes it should be clear in the SoAR that the level of due diligence applied in the assessment is commensurate to the information security classification level (Protected A, Protected B, Protected C). See the Information Security Classification Standard for a description of classification levels.

Critical System □ – Check this box if a system has been classified as critical consistent with assessments that have already occurred as part of Critical Systems Standard compliance.

Type – Select "LITE" if a decision was made to complete the SoAR only (i.e. the system is not critical and does not contain confidential or personal information.) Select "COMPREHENSIVE" if a decision was made to collect evidence, complete supporting documentation, and conduct a SoAR (i.e. the system is critical or contains confidential or personal information, or the MISO decides that a more detailed STRA activity is appropriate within their professional judgement.)

Primary Risk Evaluator – This is the person who has taken action to gather information, analyze, and document risks related to the system being assessed. Usually this is the Ministry Information Security Officer.

Owner – The person responsible for the delivery or operations of the system which is the subject of the assessment.

SoAR is confidential □ - The OCIO will maintain an inventory of all STRAs from across government for which it has been permitted to. This inventory will be helpful to ministries across government when determining whether an STRA has already been conducted for a system. If you do not want your STRA listed in the inventory due to confidentiality you need to check this box. Typically you would check this if the very knowledge of the existence of the SoAR itself could cause harm and is confidential in nature.

SoAR is shareable □ **-** Acceptance of this is helpful for transparency and to reduce redundancy, re-work, and time for others across government when completing a SoAR. Shareable SoARs can be accessed by MISOs and other approved users by searching the STRA INVENTORY site. When MISOs are able to draw on existing past assessments it helps them to think about the current assessment which they are conducting. Potentially past documented risks may be re-usable and may apply to the assessment which a MISO is working on. The ability to draw on such a pre-existing knowledge base presents the potential for significant efficiency gains. Typically, one would select not to share if the content within the SoAR could cause harm or is confidential in nature.

SoAR is Indexable □ **-** Acceptance of this is helpful for transparency and to reduce redundancy, re-work, and time for others across government when completing a SoAR. Indexable SoARs have the document title and relevant meta-data accessible by MISOs and other approved users by searching the STRA INVENTORY site.

Scope – This field indicates if the STRA conducted is at a ministry or corporate level.

Short Description – This field allows for context and explanation to be provided related to the system, an executive summary, system description, assessment description, high level findings, comments, and recommendations.

SECTION B – RISK ASSESSMENT TABLE

Purpose of section:

This section documents the risks that were identified during the assessment.

Instructions:

If more rows are needed copy from an existing row to keep drop-downs. If no risks are identified in the SoAR please provide a justification in the "System description, executive summary, and comments" box and reference the location of any existing related risk documentation.

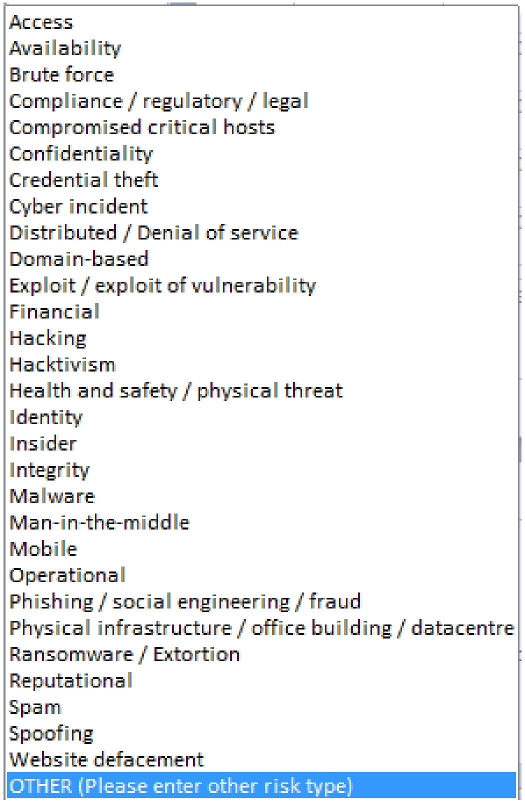
Description of fields:

Risk Ref # - This is a unique reference number within the STRA and SoAR for the risk.

Risk Name – This should in a few short words portray the gist of the risk to the reader.

Primary Risk Type – This field is intended to help categorize the nature of the risk to help the reader better understand what the risk means to the organization.

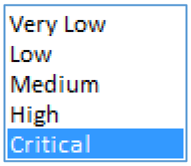
Options are provided in a drop down for this field. Select one of these options, or clear the field and enter in your own response manually.



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
Mobile
Operational
Phishing / social engineering / fraud
Physical infrastructure / office building / datacentre
Ransomware / Extortion
Reputational
Spam
Spoofing
Website defacement
OTHER (Please enter other risk type)

Risk Rating – This field is intended to provide the reader with a logical and plain language sense of how seriously they should take the risk.

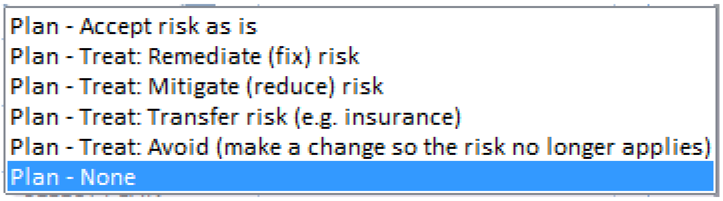
Options are provided in a drop down for this field.



Very Low
Low
Medium
High
Critical

Treatment Plan – This field is not intended to be detailed. This field is intended to provide a very high level course of action.

Options are provided in a drop down for this field.



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 provide the primary risk evaluator with a place to bring forward any information which they feel could assist the reader in better understanding the risk and or treatment. This should not be more than two sentences.

SECTION C – ACCEPTANCE

Purpose of section:

This section documents sign-offs for a STRA.

Instructions:

- Please do not remove or change the signature blocks marked “required” in the SoAR.
- Additional signature blocks may be added to address ministry needs.
- The owner is typically the “responsible person” for the system being assessed.
- The Ministry Information Security Officer is typically the “responsible person” for the assessment and the “Primary Risk Evaluator”.
- The DM, MCIO, or delegate is typically the “accountable person” who signs the SoAR. In cases where delegation occurs the delegate needs to ensure that the head of the government organization remains aware of information security risks so that they can fulfill their duty related to “reasonable security” under FIPPA legislation.
- The CISO’s signature is an acknowledgement that OCIO has received the SoAR only.
- Delegated signing must be permitted by the person you are signing on behalf of.
- Digital or printed signatures are acceptable and must be included with the SoAR.
- SoAR completion marks the completion of a Security Threat and Risk Assessment (STRA).
- SoAR completion requires all signatures.