Skymeba

ITSP.10.033 STARTER TEMPLATE · TRA

Threat and Risk Assessment

Threat modelling, vulnerability analysis, and residual-risk register for Government of Canada systems

Harry Foy

EDITION 1.0 · 2026

Threat and Risk Assessment

Threat modelling, vulnerability analysis, and residual-risk register for Government of Canada systems

EDITION 1.0 · 2026

Harry Foy

Skymeba Cybersecurity Solutions

Calgary, Canada

STARTER TEMPLATE — CUSTOMIZE FOR YOUR SYSTEM

Every heading, prompt, and field in this template is intended to be replaced, expanded, or removed to match the system being assessed. Italic text in muted grey is placeholder guidance for the author.

How to use this template

The Threat and Risk Assessment (TRA) turns the injury statements in the Statement of Sensitivity into an evidence-backed picture of what could go wrong, how likely it is, and what will be done about it. It is the artifact that lets the Departmental Security Officer make a defensible authorization decision.

This starter template follows the ITSG-33 threat-agent taxonomy and combines it with a STRIDE-style scenario structure. Every table below is intended to be edited: rows are examples that make the shape of a good entry visible. Delete the examples before signing.

A TRA is only credible if its scope matches the SSP authorization boundary and its inputs match the SoS categorization. Complete §1 with those anchors first; the rest of the assessment must trace back to them.

1 · Scope and boundaries

The scope statement here MUST match the SSP authorization boundary. Any drift will be caught by the assessor.

System name (and SoS reference)

[System name as declared in the SoS; include SoS revision date.]

Assessment window

[Start and end dates covered by this TRA.]

Categorization inherited from SoS

[e.g. Protected B / Medium / Medium.]

What is IN scope

[Enumerate components, environments, and data flows included.]

What is OUT of scope

[Explicit exclusions, with the SA&A id of the system that covers them.]

Cloud / shared-service dependencies

[CCCS Medium, tenant, common services relied upon.]

2 · Assets under assessment

List every asset a threat actor could target. Group by category so the risk register in §6 can reference them by id.

ID	Asset	Type	Owner	Notes
A-01	[Public-facing web application]	Application	[Product owner]	[Handles PB benefit records.]
A-02	[Application database]	Data store	[DBA lead]	[Encrypted at rest; TDE keys in HSM.]
A-03	[Admin console]	Application	[Ops lead]	[Restricted to admin subnet.]
A-04	[SIEM / log store]	Monitoring	[Security ops]	[12-month retention.]

3 · Threat agents considered

Use the ITSG-33 threat model as a starting point and adjust for departmental context. Delete agents that are not credible and add sector-specific ones (e.g., foreign state, insider with elevated access) where the SoS injury statements imply an elevated profile.

Agent	Level	Motivation	Relevance to this system
Unstructured external	L	Curiosity, notoriety	[Applies to public endpoints.]
Structured external	M	Financial, ideological	[Applies where PII or PB data is exposed.]
Insider (unintentional)	—	Error	[Baseline for all staff-facing components.]
Insider (malicious)	M	Grievance, financial	[Reduce with least privilege and separation of duties.]
Foreign state / APT	H	Espionage	[Assess based on program sensitivity.]
Supply-chain adversary	M	Access to downstream	[Assess against SBOM and vendor risk.]

Level: L = Low · M = Medium · H = High · — = not applicable.

4 · Threat scenarios

Write scenarios in the form: agent + action + asset → outcome. Cross-reference asset ids from §2.

ID	Scenario	Class	Assets	Preconditions
T-01	[Structured external actor exploits an unauthenticated API endpoint to enumerate PB records.]	I / D	A-01, A-02	[Public exposure; weak input validation.]
T-02	[Malicious insider with support role exports the customer table to removable media.]	I	A-02	[Broad database read grants; no DLP on endpoints.]

ID	Scenario	Class	Assets	Preconditions
T-03	[Supply-chain adversary injects a backdoor into a third-party JS dependency.]	T	A-01	[Undocumented npm dependencies; no SBOM enforcement.]
T-04	[Ransomware operator encrypts application storage and the SIEM.]	D	A-02, A-04	[Flat network; write access to backups from same domain.]
T-05				

STRIDE codes — S: Spoofing · T: Tampering · R: Repudiation · I: Information disclosure · D: Denial of service · E: Elevation of privilege.

5 · Vulnerabilities in the current implementation

Capture vulnerabilities that make one or more scenarios feasible. Reference the control failure (e.g., NIST SP 800-53 control id) where a specific control is under-implemented.

ID	Vulnerability	Related scenario(s)	Control gap
V-01	[API endpoint lacks authentication for enumeration.]	T-01	IA-2, AC-3
V-02	[No DLP or removable-media controls on support workstations.]	T-02	SC-8, MP-7
V-03	[Third-party JS dependencies not pinned or SBOM-tracked.]	T-03	SA-11, SR-3
V-04	[Backups accessible from the production admin subnet.]	T-04	CP-9, AC-6

6 · Risk register

Compute risk as Likelihood × Impact. Use the 3×3 scale below unless the department mandates a 5×5 or quantitative model.

Risk id	Scenario(s)	Likelihood	Impact	Inherent risk	Treatment
R-01	T-01	M	H	High	Mitigate: implement authN + rate limits.
R-02	T-02	L	H	Medium	Mitigate: DLP + separation of duties.
R-03	T-03	M	M	Medium	Mitigate: SBOM + dependency pinning.
R-04	T-04	L	H	Medium	Mitigate: air-gapped backups, immutable storage.

6.1 Likelihood × Impact matrix (3×3)

Likelihood: L = Rare · M = Possible · H = Likely. Impact: L = Limited injury · M = Serious injury · H = Very serious or catastrophic.

	Impact L	Impact M	Impact H
Likelihood H	Medium	High	Very High
Likelihood M	Low	Medium	High
Likelihood L	Very Low	Low	Medium

7 · Treatment plan and residual risk

For each risk, document the treatment (mitigate, transfer, avoid, accept), the specific controls to be implemented or strengthened, the owner, and the target date. Residual risk is the risk that remains AFTER treatment is applied.

Risk id	Treatment	Controls to implement	Owner	Target date	Residual risk
R-01	Mitigate	[IA-2, AC-3, SI-10]	[App team]	[YYYY-MM-DD]	Low
R-02	Mitigate	[SC-8, MP-7, PS-6]	[Sec ops]	[YYYY-MM-DD]	Low
R-03	Mitigate	[SA-11, SR-3, RA-5]	[Dev tooling]	[YYYY-MM-DD]	Low
R-04	Mitigate	[CP-9, AC-6]	[Platform]	[YYYY-MM-DD]	Low

8 · Residual risk statement for the DSO

Overall residual risk rating (after treatment)

[Low / Medium / High. Justify against the SoS injury statements.]

Recommendation to the Departmental Security Officer

[Recommend ATO / Interim ATO / Conditional / Denial. State conditions and expiry.]

Risks recommended for formal acceptance

[List any risks that will be accepted rather than mitigated, and why acceptance is appropriate.]

Monitoring and reassessment triggers

[Which changes trigger reassessment: major release, new integrations, incidents, threat-landscape shifts.]

Approvals

The signatures below confirm that the responsible parties have reviewed this document, that its contents accurately reflect the system, and that the recorded decisions are authorized.

TRA lead

Prepared the assessment and confirms the analysis is complete and evidence-backed.

Name	Signature	Date

System owner / delegate

Confirms the scope, assets, and treatment plan reflect the system as operated.

Name	Signature	Date

IT Security lead

Confirms the control gaps and treatment mapping are consistent with departmental control profiles.

Name	Signature	Date

Departmental Security Officer (DSO)

Accepts the residual risk statement in §8 or returns the assessment for further work.

Name	Signature	Date