
ITSP.10.033 STARTER TEMPLATE · SSP

# System Security Plan

Boundary, control implementation, and continuous-monitoring record for Government of Canada systems

**Harry Foy**

EDITION 1.0 · 2026

# System Security Plan

Boundary, control implementation, and continuous-monitoring record 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 System Security Plan (SSP) is the single artifact that tells an assessor what a system is, where its authorization boundary lies, and how every applicable security control is implemented. It is the anchor for the authorization decision.

This starter template covers the eight sections an ITSP.10.033 SSP is expected to contain. The heaviest section (§5, control implementation) is scaffolded family-by-family so the writer can expand each family into a control-by-control statement without having to invent the structure.

An SSP is only useful if it stays current. Section 7 captures the continuous-monitoring plan; Section 6 tracks the POA&M. Both are living records, not one-time deliverables.

## 1 · System identification

*This block is the assessor's first read. Every downstream artifact (SoS, TRA, control-implementation statements) must reference the same system name and version.*

**System name (unique across the department)**

*[ Formal name used in the departmental IT catalogue. ]*

**System acronym / short id**

*[ e.g. GCNS3-OEM2. ]*

**SSP version and date**

*[ 1.0 — YYYY-MM-DD ]*

**Departmental sponsor**

*[ Business unit that owns the outcome. ]*

**Service owner**

*[ IT lead accountable for the operational service. ]*

**Categorization (from SoS)**

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

**Authorization type sought**

*[ ATO · IATO · Conditional · Renewal. ]*

**Requested expiry / reassessment**

*[ Date the authorization needs to be renewed by. ]*

# 2 · Authorization boundary

*The boundary is what the DSO is being asked to authorize. Everything IN the boundary is assessed here; everything OUT is assessed elsewhere and inherited by reference. Drift between the boundary and the TRA scope is the most common cause of ATO rework.*

State the boundary in words first, then support it with the in-scope inventory and the inheritance table.

**Boundary statement**

*[ In prose: which components are included, which are excluded, and why. Two to four sentences. ]*

## 2.1 In-scope components

| ID | Component | Type | Environment | Owner |
|---|---|---|---|---|
| C-01 | [ Public web app ] | Application | Prod | [ App team ] |
| C-02 | [ Application API ] | Application | Prod | [ App team ] |
| C-03 | [ Application database ] | Data store | Prod | [ DBA ] |
| C-04 | [ Admin console ] | Application | Prod | [ Ops ] |

### 2.2 Inherited services and controls

*Anything not implemented directly by this system must be inherited from a service with its own authorization. Cite the ATO reference so the assessor can verify it.*

| Service | Provided by | Controls inherited | ATO reference |
|---|---|---|---|
| Cloud infrastructure | [ CCCS-authorized CSP ] | SC-7, SC-8, CP-9 (infra layer) | [ CCCS Medium ATO id ] |
| Enterprise identity | [ Departmental IdP ] | IA-2, IA-5, AC-2 (staff and admin) | [ Departmental id ] |
| SIEM and log storage | [ Enterprise security service ] | AU-6, AU-11, IR-4 (monitoring) | [ Enterprise id ] |

## 3 · System description

Explain what the system does, who uses it, and how the parts fit together. The assessor should be able to reason about the SRTM after reading this section, without asking a follow-up.

**Business purpose**

*[ What the system exists to do; the mission it supports. ]*

**User populations and volumes**

*[ Who uses it (staff, partners, public), roughly how many, and how they authenticate. ]*

**Data flow summary**

*[ Where data enters, is processed, and leaves. Reference the architecture diagram in Appendix A. ]*

**External integrations**

*[ Named systems this connects to, with the security agreement id for each. ]*

**Operating hours and availability targets**

*[ Uptime target, maintenance window, and after-hours support model. ]*

## 4 · Roles and responsibilities

*RACI at role level, not name level. Named individuals belong in the operational runbook and change as staff rotate; the SSP records the accountable role.*

| Role | Responsibility | Contact channel |
|---|---|---|
| Business owner | Accepts business risk and signs the SoS. | [ Directorate mailbox ] |
| System owner | Day-to-day authority for the system. | [ Team mailbox ] |
| System security officer (SSO) | Owns this SSP and the SRTM. | [ Security ops queue ] |
| DSO | Grants and revokes ATOs on behalf of the department. | [ DSO office ] |
| Privacy officer | Signs off on privacy controls and PIAs. | [ Privacy office ] |
| Assessor | Independently verifies control implementation. | [ SA&A queue ] |

## 5 · Security control implementation

*This is the heart of the SSP. For every control in the profile, record: who implements it, how it is implemented, and where the evidence lives. Inherited controls state the source and stop there.*

The subsections below give one row per NIST SP 800-53 family as a scaffold. Replace the placeholders with a paragraph per control from the applicable ITSG-33 profile. Detail should be sufficient for an assessor to plan a test.

| Family | Name | Implementation summary |
|---|---|---|
| AC | Access Control | [ How identity and role are enforced across the boundary. Reference IdP, RBAC model, and privileged access workflow. ] |
| AT | Awareness and Training | [ Role-based training for staff and privileged users; frequency and evidence source. ] |
| AU | Audit and Accountability | [ What is logged, retention, and how logs flow to the enterprise SIEM. Reference AU-6 review cadence. ] |
| CA | Assessment, Authorization, and Monitoring | [ Assessment path, ATO type, continuous monitoring cadence, and reporting to the DSO. ] |
| CM | Configuration Management | [ Baseline sources, change control process, and drift detection. ] |
| CP | Contingency Planning | [ RTO/RPO targets, backup strategy, DR test cadence, and last successful test date. ] |
| IA | Identification and Authentication | [ MFA posture for staff, admins, and non-person entities; credential rotation. ] |
| IR | Incident Response | [ IR plan location, tabletop cadence, and integration with CCCS reporting obligations. ] |
| MA | Maintenance | [ Patch cadence, maintenance windows, and remote-maintenance safeguards. ] |
| MP | Media Protection | [ Media handling for Protected data, sanitization, and disposal evidence. ] |
| PE | Physical and Environmental Protection | [ Facility inheritance from the CSP; office controls that apply to admins. ] |
| PL | Planning | [ This SSP, the SoS, the TRA, and the SRTM — with owners and review cadence. ] |
| PM | Program Management | [ Departmental security program references. ] |

| Family | Name | Implementation summary |
|---|---|---|
| PS | Personnel Security | [ Screening levels required per role, and how they are verified. ] |
| PT | PII Processing and Transparency | [ PIA status, transparency notices, and consent handling. ] |
| RA | Risk Assessment | [ Reference to the TRA and vulnerability-scan cadence. ] |
| SA | System and Services Acquisition | [ SDLC controls, third-party dependency handling, and SBOM enforcement. ] |
| SC | System and Communications Protection | [ Encryption in transit and at rest; network segmentation; boundary protection. ] |
| SI | System and Information Integrity | [ Input validation, integrity monitoring, and vulnerability remediation SLAs. ] |
| SR | Supply Chain Risk Management | [ Vendor risk process, contract clauses, and dependency provenance. ] |

*Detailed control-by-control implementation statements belong in the SRTM workbook (one row per control). This table is the SSP-level orientation for the family; the SRTM is where each control statement lives.*

## 6 · Plan of action and milestones (POA&M)

Every deficiency the assessor flags, or that the team self-identifies, gets an entry here with an owner, a target date, and a residual-risk statement while it is open.

| POA&M id | Deficiency | Owner | Target date | Residual risk |
|---|---|---|---|---|
| P-01 | [ Description of the gap. ] | [ Role or team ] | [ YYYY-MM-DD ] | [ L / M / H ] |
| P-02 | | | | |
| P-03 | | | | |

## 7 · Continuous monitoring plan

Describe how the control posture is kept current between authorizations. Cite the cadence and the evidence source for each activity.

| Activity | Cadence | Owner | Evidence source |
|---|---|---|---|
| Vulnerability scanning (authenticated) | Weekly | [ Sec ops ] | [ Scanner tenant ] |
| Configuration drift review | Monthly | [ Platform ] | [ CM tooling ] |
| Log review (AU-6) | Weekly | [ Sec ops ] | [ SIEM saved search ] |
| Access recertification | Quarterly | [ Identity ] | [ IdP report ] |
| Tabletop exercise | Annual | [ IR lead ] | [ Exercise report ] |
| DR test | Annual | [ Platform ] | [ DR report ] |

## 8 · Appendices

The SSP itself stays short. Detail belongs in appendices, each of which is a separately versioned document referenced by this SSP.

- Appendix A — Architecture and data-flow diagrams (versioned SVG or PDF).
- Appendix B — System Requirements Traceability Matrix (SRTM) workbook.
- Appendix C — Threat and Risk Assessment (TRA).
- Appendix D — Statement of Sensitivity (SoS).
- Appendix E — Privacy Impact Assessment (PIA), if in scope.
- Appendix F — Incident-response runbook.
- Appendix G — Contingency and disaster-recovery plan.
- Appendix H — List of interconnection security agreements.

# 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.

**System security officer (SSO)**

*Prepared this SSP and confirms the control-implementation statements are current.*

| Name | Signature | Date |
| --- | --- | --- |
| | | |

**System owner / delegate**

*Confirms the boundary, description, and roles reflect the system as operated.*

| Name | Signature | Date |
| --- | --- | --- |
| | | |

**IT Security lead**

*Confirms the control profile is appropriate for the categorization and that inheritance claims are valid.*

| Name | Signature | Date |
| --- | --- | --- |
| | | |

**Departmental Security Officer (DSO)**

*Grants the authorization based on this SSP, the TRA, and the SoS.*

| Name | Signature | Date |
| --- | --- | --- |
| | | |