Skymeba

SKYMEBA CYBERSECURITY SOLUTIONS

From ITSG-33 to ITSP.10.033

A Practitioner's Guide to Security Assessment & Authorization for the Government of Canada

Harry Foy

EDITION 1.0 · 2026

From ITSG-33 to ITSP.10.033

A Practitioner's Guide to Security Assessment & Authorization for the Government of Canada

Edition 1.0 — 2026

Author: Harry Foy

Publisher: Skymeba Cybersecurity Solutions

Calgary, Alberta, Canada

This book is a professional interpretation of publicly available guidance. It is not legal advice and does not represent the position of the Treasury Board of Canada Secretariat, the Communications Security Establishment, or the Canadian Centre for Cyber Security.

PRINTED AND DISTRIBUTED IN CANADA

Contents

Chapter 1 — Why ITSG-33 Is Being Superseded and What ITSP.10.033 Changes

For roughly a decade, IT security risk management in the Government of Canada revolved around ITSG-33: IT security risk management — A lifecycle approach, and specifically its Annex 3A control catalogue derived from NIST SP 800-53 Rev. 4, and its Annex 4 baseline profiles such as the Protected B / Medium integrity / Medium availability ("PBMM") profile.

In 2026 the Canadian Centre for Cyber Security (CCCS) began transitioning departments to a successor document — ITSP.10.033: Security and privacy controls and assurance activities catalogue, part of the new *Cyber security and privacy risk management series*. The new catalogue is issued under the authority of the Head of CCCS and consolidates security *and* privacy controls along with the *assurance activities* used to evaluate them (CCCS ITSP.10.033 Foreword).

1.1 What actually changes

At a structural level ITSP.10.033 keeps the NIST SP 800-53 family/control lineage familiar to ITSG-33 users but introduces four material differences (CCCS ITSP.10.033 PDF):

1. **Security and privacy in one catalogue.** Privacy controls that used to be handled through separate TBS instruments are now integrated alongside security controls, mirroring the direction of NIST SP 800-53 Rev. 5.
2. **Assurance activities are catalogued next to the control.** Each control ships with a description of the engineering work, documentation content, and assessment tasks required to demonstrate the control is implemented and effective. Assessors

and practitioners work from the same reference (Public Services and Procurement Canada's CPCSC Level 1 guidance explicitly points at ITSP.10.033 assurance activities as the yardstick).

3 **Suggested organizational profiles replace Annex 4 baselines.** A "medium impact" organizational profile — ITSP.10.033-01 — plays the same role the old PBMM profile did but is authored as a *starting recommendation* rather than a mandatory baseline, in line with the departmental-risk-ownership model.

4 **Common services, implementer roles, and privacy assignments are explicit.** ITSP.10.033 distinguishes controls that are the responsibility of a *common service provider* (typically SSC or a cloud provider), an *organization*, or a *system*, and identifies whether an activity is implementer- or assessor-oriented (Verity GRC transition summary).

The lifecycle process — categorize, select, implement, assess, authorize, monitor — is unchanged in spirit; what changes is the catalogue you cite, the phrasing of the requirements, and how privacy is folded into the same package (CCCS ITSP.10.033 landing page).

1.2 What does not change

- The Treasury Board Policy on Government Security and Directive on Security Management remain the top of the policy stack. SA&A is an *implementation* of those obligations.
- The **Departmental Security Officer (DSO)** remains the accountable senior official for security management within the department, with the deputy head as ultimate accountable executive.
- Cloud-specific guidance in ITSP.50.105 — Guidance on cloud security assessment and authorization and the GC Cloud Security Risk Management Approach continue to apply.

- ITSG-33 has not been withdrawn as of publication; departments will run *both* references during transition. Cite ITSP.10.033 for new work and identify equivalent ITSG-33 controls in the same row of your traceability matrix during the transition window.

1.3 How to read this book

Every chapter has three lenses:

- **Practitioner** — what to build and produce.
- **Assessor** — what to examine, interview, and test, and how to write findings that survive appeal.
- **Recipient / DSO** — what to look for before signing an Authority to Operate (ATO) or accepting residual risk.

Chapter 10 stitches the lenses together on a single Azure Protected B example.

Chapter 2 — The SA&A Lifecycle in the GC — End to End

The GC lifecycle is described most concretely in ITSG-33 Annex 2 — Information System Security Risk Management Activities as the "Information System Security Implementation Process" (ISSIP), and it maps almost one-to-one to the NIST SP 800-37 Rev. 2 Risk Management Framework.

2.1 The six phases

Phase	GC term (ITSG-33 / ITSP.10.033)	NIST RMF equivalent	Primary output
1	Initiation & categorization	Prepare + Categorize	Statement of Sensitivity (SoS), business needs for security
2	Security control selection & tailoring	Select	Tailored control set / SRTM
3	Design, build, implement	Implement	System Security Plan (SSP), design artifacts
4	Assessment	Assess	Security Assessment Plan (SAP), Security Assessment Report (SAR)
5	Authorization	Authorize	ATO letter, PoA&M, residual-risk acceptance

Phase	GC term (ITSG-33 / ITSP.10.033)	NIST RMF equivalent	Primary output
6	Continuous monitoring	Monitor	ConMon reports, reassessment, change control

2.2 Entry criteria for each phase

The most common source of grief in GC SA&A engagements is starting a phase before the prior one is closed. Concretely:

- Do not draft an SRTM (phase 2) before the SoS and categorization are signed by the business owner. The categorization drives everything downstream.
- Do not begin assessment (phase 4) before the SSP is *implementation-complete* and traceable to the SRTM — assessors have no basis to test otherwise.
- Do not present a SAR to a DSO (phase 5) that has open "assessment not performed" findings; convert them either to findings or to PoA&M items with justification.

2.3 Typical durations

For a Protected B system of moderate complexity in a cloud tenant, realistic durations are:

Phase	Practitioner effort	Elapsed time
Categorization + SoS	1–2 weeks	2–4 weeks (business sign-off)
Selection & tailoring	2–3 weeks	3–6 weeks
Implementation & SSP drafting	Runs with project delivery	Months, tied to release plan
Assessment	3–6 weeks assessor time	6–10 weeks with iterations

Phase	Practitioner effort	Elapsed time
Authorization	1 week paperwork	2–6 weeks decision cycle

These are guidance numbers, not commitments. The realistic risk is compression of assessment because delivery ran long.

Chapter 3 — Governance, Roles, and Responsibilities

The GC governance model overlaps with, but is not identical to, US federal RMF or ISO 27001 governance. The TBS Directive on Security Management assigns the accountabilities described below.

3.1 Accountable roles

- **Deputy Head.** Ultimate accountability for departmental security and for accepting residual risk on behalf of the department.
- **Departmental Security Officer (DSO).** Senior official who leads the departmental security program and, in most departments, holds delegated authority to sign the ATO for systems under a threshold. Reports on residual risk to the deputy head.
- **Chief Information Officer (CIO) / Chief Security Officer (CSO).** Owns IT and security policy execution and, jointly with the DSO, the risk view for enterprise services.
- **Business Owner / Program Authority.** Owns the *information* and the business outcome; owns the Statement of Sensitivity, the injury assessment, and — critically — the tolerance for residual risk.
- **System Owner / Project Authority.** Owns the *system* through its lifecycle; produces or commissions the SSP, ensures controls are implemented, and remediates PoA&M items.

3.2 Delivery and assessment roles

- **Security Practitioner / Security Architect.** Selects and tailors the control set, defines the authorization boundary, produces the SSP, coordinates evidence collection.

- **Security Assessor.** Independent from the delivery team; executes the SAP against the SSP, produces the SAR, applies professional interpretation, and does *not* make the authorization decision.
- **Independent Assessor / Third-Party Assessment Organization (3PAO equivalent).** For higher-impact systems or for cloud service providers, an independent assessor is required. The CCCS CSP IT Security Assessment Process (ITSM.50.100) describes how CCCS itself assesses cloud providers.
- **Privacy Function (ATIP / Privacy Office).** Reviews personal-information handling, PIA obligations, and — under ITSP.10.033 — the privacy control activities embedded in the catalogue.

3.3 Approving parties in typical deliverables

Deliverable	Drafted by	Reviewed by	Approved by
Statement of Sensitivity (SoS)	Practitioner + Business Owner	DSO, Privacy	Business Owner
SRTM / Tailored control set	Practitioner	Assessor (peer review), Architecture	System Owner + DSO delegate
System Security Plan (SSP)	Practitioner	Assessor, Operations, Privacy	System Owner
Security Assessment Plan (SAP)	Assessor	Practitioner (for scope), System Owner	DSO or DSO delegate
Security Assessment Report (SAR)	Assessor	Practitioner (for factual accuracy)	DSO for acceptance of findings
PoA&M	Practitioner	Assessor, Operations	System Owner (creates); DSO (accepts)

Deliverable	Drafted by	Reviewed by	Approved by
Authority to Operate (ATO) letter	DSO office	CIO, Privacy	**DSO** (or delegated authorizer)

Appendix A restates this as a single RACI-style matrix.

Chapter 4 — Defining the Authorization Boundary

4.1 Why the boundary matters more than anything else

Everything else — categorization, control selection, evidence scope, cost, timelines — cascades from the authorization boundary. NIST SP 800-37 Rev. 2 defines it as "all components of an information system to be authorized for operation by an authorizing official" (NIST 800-37 r2; NIST glossary). ITSP.10.033 adopts the same construct.

A boundary that is drawn too wide inflates evidence collection and slows the ATO; drawn too narrow, it hides real risk and later gets rejected by the DSO or independent assessor.

4.2 A repeatable method

1. **Start with the data flow.** For each unique category of information the system creates, receives, stores, transmits, or destroys, list the components involved. This is the "data-centric" approach the FedRAMP Authorization Boundary Guidance uses and it works well in Canada.
2. **Classify each component.** For every component, mark it as *in boundary*, *in scope but externally authorized* (e.g., a Protected B-authorized SaaS), or *out of scope* (e.g., corporate email used only for administrative notifications).
3. **Draw the diagram.** A one-page authorization boundary diagram must exist. It shows components, trust zones, ingress/egress, and identity boundaries. If it does not fit on one page, the boundary is probably wrong.

4 **Enumerate interconnections.** Every external interconnection needs a documented agreement (ISA, MOU, or contractual clause) and a control expectation from the other side.

5 **Reconcile with inventory.** The boundary diagram, the CMDB, and the cloud subscription/tenant inventory must reconcile. Discrepancies are a common assessor finding.

4.3 Cloud-specific considerations

Under ITSP.50.105, the boundary explicitly includes the customer-managed layer of the cloud service (subscriptions, resource groups, IAM, key vaults, network resources) *and* the inherited controls from the CSP that has itself been through the CCCS CSP assessment program.

For Azure, the CSP boundary is what Microsoft has certified under CCCS Medium at Protected B — documented in the Microsoft compliance offerings for CCCS Medium and Canada Protected B. Everything above that shared-responsibility line is your boundary.

4.4 Common boundary mistakes

- Treating the entire Azure tenant as "in boundary" when only a single subscription is used by the system.
- Forgetting the CI/CD pipeline, the artifact registry, and secrets stores that touch production.
- Excluding a monitoring or SIEM tenant that reads production logs — if it can read them, it is in scope.
- Excluding the administrative jumpbox used only "occasionally".

Chapter 5 — Categorization, Profile Selection, and Tailoring an SRTM

5.1 Categorization and the Statement of Sensitivity

Categorization in the GC is expressed as a triplet — *confidentiality, integrity, availability* — and mapped to *injury levels*. The most common target for departmental cloud systems is **Protected B / Medium integrity / Medium availability (PBMM)**, described in the GC Security Control Profile for Cloud-Based IT Services and in ITSM.50.109.

The Statement of Sensitivity (SoS) is the artifact where the business owner records the injury analysis. Under ITSP.10.033 the SoS also records privacy sensitivity (personal information categories, PIA status) because privacy controls now live in the same catalogue.

5.2 Selecting a profile

Under ITSG-33, you selected an Annex 4 profile such as Profile 1 — PBMM. Under ITSP.10.033, the equivalent is a *suggested organizational profile*. For medium-impact systems, use the ITSP.10.033-01 medium-impact profile as the starting point and tailor from there.

5.3 The SRTM — the Canadian answer to the ISO 27001 Statement of Applicability

The Security Requirements Traceability Matrix is, functionally, the GC's Statement of Applicability (SoA) plus its implementation and testing records. FedRAMP publishes the canonical SRTM shape in the High SRTM and Moderate SRTM templates — a workable starting shape for GC work.

A workable SRTM for a Protected B system has, at minimum, these columns:

Column	Purpose
ITSP.10.033 control ID	New catalogue reference
ITSG-33 equivalent	Bridge during transition
Control text (parameterized)	Departmental values inserted
Applicability	Applicable / Not applicable + rationale
Responsibility	Common service / Organization / System / Shared
Implementer role	e.g., Cloud platform team, App team, SecOps
Implementation statement	How, in prose, the control is met
Evidence pointer	Location of examine/interview/test artifacts
Assurance activity result	Satisfied / Partially satisfied / Not satisfied / Not applicable
Risk if not satisfied	For PoA&M generation

Tailoring vocabulary

- **Scoping decision.** A control is not applicable because a technology or condition does not exist (e.g., no wireless controls when the system has no wireless components).

- **Parameterization.** A control has organization-defined values (frequency, duration, roles) that you set — record the value and the rationale.
- **Compensating control.** A control cannot be met literally, and an alternative achieves equivalent risk reduction — record the alternative *and* the risk analysis.
- **Common control inheritance.** The control is provided by a common service (SSC network, Entra ID tenant, CSP infrastructure) — record the source, the evidence handoff, and the inheritance limits.

Comparison to other frameworks

Concept	ITSP.10.033 / GC	ISO 27001	NIST 800-53 / FedRAMP	SOC 2
Scope statement	Authorization boundary	ISMS scope	System boundary	System description
Applicability register	SRTM	Statement of Applicability	SRTM (SAR Appendix B)	Description of controls in SOC 2 report
Baseline	ITSP.10.033-01 medium profile	Annex A + tailoring	Low / Moderate / High baselines	Trust services criteria (no baseline)
Findings register	SAR + PoA&M	Nonconformity register + CAPA	SAR + POA&M	Exceptions in Section 4
Authorization	DSO ATO	Certification decision	AO ATO	Auditor opinion (Type I/II)

Chapter 6 — The System Security Plan (SSP) and Supporting Documentation

The SSP is the single, load-bearing document. Assessors work from it, DSOs decide on it, and continuous monitoring updates it.

6.1 What must be in the SSP

At minimum:

1. **System identification.** Name, unique ID, owner, categorization, boundary diagram, hosting model.
2. **Business context.** Users, information categories, injury assessment (SoS reference), sensitivity of personal information.
3. **Architecture description.** Logical, physical, network, identity, and data views. Named components and versions.
4. **Environments.** Production, staging, test, dev — noting which are in the authorization boundary.
5. **Interconnections.** External systems, agreements in place, controls expected of each.
6. **Control implementation statements.** One per applicable control, describing *how* the control is met (not restating the control text).
7. **Roles and responsibilities.** Who operates each control day-to-day.
8. **Related documents.** SoS, threat and risk assessment (TRA), PIA, DR/BCP plan, incident response plan, configuration management plan, contingency plan tests, vulnerability management plan.

6.2 Supporting documents

- **Threat and Risk Assessment (TRA).** Uses the Harmonized TRA methodology as its base. The TRA is where system-specific threats are analyzed; the SSP references its conclusions.
- **Privacy Impact Assessment (PIA).** Required when personal information is handled; the assessor may reuse PIA findings for the privacy controls in ITSP.10.033.
- **Configuration Management Plan.** Baselines, change control, patch cadence.
- **Contingency / DR Plan and test evidence.** BCP tests, RTO/RPO measurements.
- **Incident Response Plan.** Roles, escalation to the departmental CSIRT, notification obligations.
- **Continuous Monitoring Plan.** What is monitored, how often, thresholds for reassessment.

6.3 Documentation quality tests

An SSP that will survive assessment answers *yes* to all of the following:

- Can a stranger read the SSP and reproduce the boundary diagram from the text?
- Does every control implementation statement name a system, a process, or a person — not just "the team"?
- Is every "as required" or "as needed" phrase replaced with a defined frequency?
- Does every reference to another document give a version and a date?

Chapter 7 — Assurance Activities: Examine, Interview, Test

ITSP.10.033's most useful addition to daily practice is that it *ships assurance activities alongside every control*. The three activity types are the same as NIST SP 800-53A (which ITSG-33 practitioners already borrow from):

- **Examine** — review documents, records, mechanisms, activities.
- **Interview** — talk to individuals or groups performing the control.
- **Test** — exercise the control and observe the outcome.

The CCCS ITSP.10.033 PDF describes assurance activities as "engineering tasks, documentation content requirements, and assessment tasks" — meaning they inform *both* the implementer's build and the assessor's test.

7.1 Building the SAP

The Security Assessment Plan is the assessor's operating document. It should:

- Restate the boundary (and confirm it against inventory).
- List the applicable controls and, for each, the assurance activities in scope.
- Identify the assessment sample — for controls affecting many components, which components will be examined or tested.
- Identify constraints — production windows, data sensitivity limits on test data, red-team boundaries.
- Identify the assessment team, their independence declaration, and their access requirements.

7.2 Evidence quality

Evidence is only useful if it is *authentic, contemporaneous, complete, and reproducible*:

- **Authentic.** Screenshots include the system chrome, hostname, and user; exports include the query used and the run timestamp.
- **Contemporaneous.** Collected within the assessment window, not "we did this six months ago".
- **Complete.** Covers the full scope claimed. A patch report that lists 10 servers when the boundary has 60 is not complete evidence.
- **Reproducible.** The assessor could re-run the same query and get the same result modulo time-based drift.

7.3 Professional interpretation vs. personal opinion

Assessors are paid for professional interpretation. Two guardrails keep interpretation from sliding into opinion:

1. **Anchor every conclusion in a control statement, an assurance activity, and specific evidence.** If a finding cannot be traced to those three, it is opinion.
2. **Use a "reasonable practitioner" test.** Would a reasonably experienced practitioner reach the same conclusion given the same evidence? If not, the finding is either mis-scoped or under-evidenced.

Assessors write findings, not designs. It is legitimate to note that "the current implementation of AC-2 does not evidence periodic account review at the parameterized frequency"; it is not the assessor's role to prescribe *which* tool the department should adopt.

Chapter 8 — The Security Assessment Report (SAR), Residual Risk, and PoA&M

8.1 What a SAR contains

At minimum, in the GC context and consistent with the FedRAMP SAR template-Template.docx):

- Executive summary with an unambiguous statement of assessment outcome.
- Scope, boundary, and sample confirmation.
- Assessment methodology — including any deviations from the SAP.
- Findings, each with: control ID, assurance activity, evidence reference, observed condition, expected condition, risk statement, and recommended risk response.
- Aggregate residual risk narrative — the "so what" for the DSO.
- PoA&M register (or reference to it).
- Appendices — the completed SRTM with per-control results, the evidence catalogue, and interview notes.

8.2 Findings and their disposition

Every finding has one of four fates:

1. **Corrected before authorization.** Practitioner produces new evidence; assessor validates; SAR is updated.
2. **Accepted as PoA&M.** Recorded with owner, milestones, and target date. DSO accepts the residual risk for the interim.

3 **Risk accepted permanently.** For findings the department chooses not to remediate, with rationale and business owner sign-off.

4 **Escalated.** For findings whose risk exceeds the DSO's delegation — see Chapter 9.

8.3 The PoA&M

The Plan of Action and Milestones is the ledger of unfinished business. Structurally it borrows from NIST SP 800-37 (which established the SAR + PoA&M pattern — see NIST SP 800-37 r2) and the ITSG-33 Annex 3A control CA-5 (Plan of Action and Milestones), which requires the organization to develop, maintain, and update a PoA&M for the information system (Annex 3A).

A workable PoA&M has:

Field	Notes
Finding ID	Same as SAR
Control(s)	ITSP.10.033 IDs
Description	Observed vs. expected condition
Risk rating	Using an agreed rubric (Appendix C)
Owner	Named individual, not a team
Planned remediation	Concrete steps
Milestones and dates	Interim checkpoints, not just a final date
Compensating measures	What reduces risk *in the interim*
Status	Open, in progress, deferred, closed
Closure evidence	Reference to re-test evidence

Who does what:

- **Practitioner / System Owner** creates the PoA&M items and drives remediation.

- **Assessor** validates closure evidence and re-tests.
- **DSO** accepts risk on open items and re-examines at each ConMon cycle.

Chapter 9 — The Authorization Decision — What a DSO Actually Decides

9.1 The decision, framed correctly

The DSO does not decide whether the system is "secure". The DSO decides whether the **residual risk** presented by the SAR is acceptable for the department to bear, given the business value of the system and the alternatives. This mirrors the NIST SP 800-37 authorization decision but is exercised under GC accountabilities described in the TBS Directive on Security Management.

9.2 Inputs the DSO should demand

Before signing:

1. A complete SAR with an unambiguous overall finding.
2. A PoA&M with named owners and dates.
3. A business-owner acknowledgement of the residual risk.
4. A privacy sign-off if personal information is involved.
5. Any prior-authorization dependencies (inherited controls from SSC, from the CSP, from a shared identity platform).

9.3 The DSO's options

- **Authority to Operate (ATO).** Full authorization for a defined period, typically 3 years, subject to continuous monitoring.
- **Interim Authority to Operate (IATO) / Conditional ATO.** Time-bounded authorization contingent on named PoA&M items

closing by defined dates. Useful when a system must go live before all findings are resolved.

- **Denial of Authorization.** Risk is not acceptable; the system does not go into production. Rare but must remain a live option — a DSO who "always signs" provides no assurance.
- **Escalation.** Where risk exceeds the DSO's delegated authority, the deputy head must decide; where risk touches other departments (SSC dependencies, shared services), TBS may be consulted.

9.4 How to reason about "accept or not accept"

A practical decision framework:

1. **Is the risk** *understood***?** If findings are vague, send them back before deciding.
2. **Is the risk** *quantifiable in business terms***?** Translate technical findings into potential injury to Canadians, to the Crown, or to the department's mandate.
3. **Is it** *bounded***?** Are there dates by which risk will be reduced?
4. **Is it** *mitigated in the interim***?** What compensating controls are in place *now*?
5. **Is the** *business value proportionate***?** A high-value citizen service can rationally accept more risk than an internal convenience tool.
6. **Is the department the** *right risk owner***?** Some risks belong to a common-service provider (SSC, Entra ID tenant owner, CSP) and should be escalated rather than accepted locally.

Document the reasoning in the ATO letter. A one-paragraph rationale for each accepted high-risk finding is a good habit.

Chapter 10 — Worked Example: A Protected B Web Application on Microsoft Azure

The example we will use for the rest of the book is deliberately common: a **departmental case-management web application** that stores Protected B personal information and integrates with SSC network services and departmental Entra ID. This is representative of the kind of system many departments run on Azure at CCCS Medium (Microsoft CCCS Medium offering; Canada Protected B offering).

10.1 The system

- **Name.** DEPT Case Management System ("DCMS").
- **Purpose.** Officers intake, triage, and manage citizen cases containing Protected B personal information.
- **Users.** ~500 internal officers and managers. No public interface. Read-only integration to a departmental data warehouse.
- **Categorization.** Protected B / Medium integrity / Medium availability (PBMM). Target profile: ITSP.10.033 medium-impact organizational profile (ITSP.10.033-01).

10.2 Architecture summary

- **Front end.** Azure App Service (Linux, containerized), fronted by Azure Front Door with WAF.
- **API layer.** Azure Container Apps in a dedicated VNet, private endpoints only.

- **Data.** Azure SQL Database (business-critical tier) with Transparent Data Encryption and customer-managed keys in Azure Key Vault (HSM-backed).
- **Storage.** Azure Storage (private endpoints) with immutable blob policy for case attachments.
- **Identity.** Departmental Entra ID tenant with Conditional Access, PIM for privileged roles, workload identities for services.
- **Networking.** Hub-and-spoke; ingress via Azure Front Door with WAF; egress via Azure Firewall; SSC-provided transit for on-prem interconnect.
- **Observability.** Azure Monitor + Log Analytics + Microsoft Sentinel; logs forwarded to the departmental SIEM.
- **CI/CD.** Azure DevOps with protected branches, signed builds, artifact registry, and OIDC federation to Azure (no long-lived secrets).

10.3 Authorization boundary

In boundary: Azure subscription(s) hosting DCMS resources, the associated Log Analytics workspace, the Key Vault, the Azure DevOps project used to build and deploy DCMS, and the tenant's Conditional Access policies scoped to DCMS.

Inherited (common service): Azure platform controls under CCCS Medium; Entra ID tenant controls; SSC transit and DNS; departmental SIEM.

Out of boundary: Corporate email, general-purpose collaboration tools not integrated with DCMS.

10.4 Shared-responsibility summary

Layer	Owner	Evidence source
Physical, hypervisor, hardware	Microsoft	Microsoft's CCCS Medium letter and associated attestations (CCCS Medium)
Platform services (App Service, SQL, Key Vault)	Microsoft (service) + department (configuration)	Microsoft attestations + Azure Policy compliance reports
Guest OS in containers, application code	Department	Build pipeline, SCA reports, patch logs
Data, identity, keys, monitoring config	Department	Entra ID reports, Key Vault access policies, Azure Monitor rules

Chapter 10b — Worked Example: A Protected B Microsoft 365 Tenant

The second worked example is deliberately different from DCMS: a **departmental Microsoft 365 tenant** ('DEPT-M365') hosting Exchange Online, SharePoint Online, OneDrive for Business, Teams, and Purview, storing and processing information up to **Protected B**. Many departments now sit on a Microsoft cloud identity and productivity platform, and the SA&A challenges are meaningfully different from those of a single custom application — the boundary is broader, the inheritance is heavier, and identity and information-protection controls do most of the work.

Microsoft's CCCS Medium offering and Canada Protected B offering both apply to in-scope Microsoft 365 services; the department retains full responsibility for the *tenant configuration*.

10b.1 The system

- **Name.** DEPT Microsoft 365 Tenant ('DEPT-M365').
- **Purpose.** Departmental email, document collaboration, file storage, meetings, and information protection.
- **Users.** ~5,000 internal employees and cleared contractors, all onboarded through departmental HR.
- **Categorization.** Protected B / Medium integrity / Medium availability (PBMM) at the tenant level; specific SharePoint sites can be raised to Protected B / High integrity by policy where mandated by business need.
- **Target profile.** ITSP.10.033-01 medium-impact organizational profile.

10b.2 In-scope services

- **Identity.** Microsoft Entra ID (P2), Entra Conditional Access, Entra PIM, Entra ID Protection, Entra Verified ID (where used).
- **Productivity.** Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams (including Teams Phone if enabled), Microsoft 365 Apps for Enterprise.
- **Security and compliance.** Microsoft Defender for Office 365 Plan 2, Defender for Endpoint P2, Defender for Cloud Apps, Microsoft Purview (Information Protection, Data Lifecycle Management, DLP, Insider Risk Management, Communication Compliance, eDiscovery Premium, Audit Premium).
- **Device management.** Microsoft Intune, Windows Autopilot.
- **Federation and B2B.** Departmental federation to Government of Canada trust broker or partner tenants as applicable.

10b.3 Authorization boundary

In boundary:

- The departmental Microsoft 365 tenant, including all licensed services listed above.
- The Entra ID tenant hosting user, guest, and workload identities that access DEPT-M365 data.
- The Intune tenant and enrolled devices used to access Protected B information.
- The Purview compliance boundary (labels, DLP policies, audit workspace).
- Admin tooling with tenant privileges: PIM, Privileged Access Management (PAM), tenant management PowerShell endpoints, and any 'Cloud Solution Provider' delegated access.
- Third-party SaaS applications granted OAuth consent to tenant data (a common oversight).

Inherited (common service):

- Microsoft's CCCS Medium controls covering the service and infrastructure layer (CCCS Medium).
- SSC transit and DNS where the department uses SSC network services to reach Microsoft's Canada regions.

Out of boundary (but adjacent — document interfaces):

- Personal devices under BYOD when the department has chosen not to allow them.
- Third-party unified-communications tools not integrated with Teams.

10b.4 Shared-responsibility summary

Layer	Owner	Evidence source
Datacenters, hypervisor, service software	Microsoft	CCCS Medium attestation
Service configuration (Exchange, SharePoint, Teams, Purview)	Department	Config exports (Set-* cmdlet outputs, Purview policy JSON)
Identity: users, groups, roles, CA, PIM	Department	Entra ID exports and sign-in logs
Data: classification, labels, DLP, retention	Department	Purview label and policy definitions, DLP incident reports

Layer	Owner	Evidence source
Devices: enrollment, compliance, hardening	Department	Intune device compliance reports and configuration profiles
Third-party app consent and workload identities	Department	Enterprise app inventory; consent policies

10b.5 Boundary and inheritance pitfalls unique to M365

- **The 'tenant' is not the boundary — the** *configuration* **is.** Two departments can license identical services and end up with wildly different risk postures. Evidence must exist at the configuration level, not at the licensing level.
- **Guest and external identities cross the boundary constantly.** B2B guests, cross-tenant access settings, and external Teams federation must be enumerated and controlled. Cross-tenant access policies are configuration evidence.
- **OAuth consent is a shadow authorization path.** Any user- or admin-consented third-party app has access to tenant data at whatever scopes were granted. A tenant that allows user consent to any app has effectively delegated authorization to end users. Evidence: consent policies, enterprise app inventory, and a periodic review record.
- **Purview labels are only as strong as the labeling behavior.** A label taxonomy on paper is not evidence; label application coverage (percentage of documents labeled) is.

- **eDiscovery and Insider Risk carry their own access risks.** Investigators can read otherwise restricted content. PIM plus audit review of Compliance role activations is expected.

10b.6 Control-by-family notes specific to M365

The general Azure evidence guidance in Chapter 11 applies; the M365 nuances are:

- **AC — Access Control.** RBAC lives in Entra ID (directory roles), inside individual services (Exchange RBAC, SharePoint site permissions), and in Purview. Evidence must cover *all three* planes, not just Entra ID roles. AC-2 requires access reviews for privileged directory roles, for Compliance and Security roles, and for site collection administrators on high-sensitivity sites.
- **AT — Awareness and Training.** DEPT-M365 users need training on labels, DLP, phishing, and Teams information handling. Purview Communication Compliance and Attack Simulation Training in Defender for Office 365 produce evidence.
- **AU — Audit and Accountability.** Purview Audit (Premium) provides tenant-wide audit with extended retention. Evidence includes Audit search results reproduced with query parameters, and the retention policy configuration.
- **CA — Assessment, Authorization, and Monitoring.** Interconnections here are tenant-to-tenant (cross-tenant access settings), tenant-to-third-party SaaS (Enterprise apps), and tenant-to-on-prem (Exchange hybrid, SharePoint hybrid, Entra Connect). Each is a CA-3 interconnection.
- **CM — Configuration Management.** Configuration is the substance of the ATO for a tenant like this. Prefer declarative config (Microsoft365DSC, Intune configuration profiles) over portal drift. Evidence includes IaC repository history and Intune compliance reports.
- **CP — Contingency Planning.** Microsoft provides service continuity; the department is responsible for *data* continuity. Evidence

includes Exchange Online mailbox retention configuration, SharePoint versioning and retention, Preservation Hold library configuration, and — for the highest sensitivity workloads — third-party backup for M365 with restore test evidence.

- **IA — Identification and Authentication.** Phishing-resistant MFA (FIDO2 / Windows Hello for Business / certificate-based) for privileged roles is the current expectation. Legacy authentication protocols must be blocked; evidence is the Conditional Access policy plus Entra sign-in logs showing zero legacy-auth successes.
- **IR — Incident Response.** Defender for Cloud Apps and Defender XDR are the primary detection surface. Sample incidents with disposition, and integration to the departmental CSIRT, are expected evidence.
- **MP — Media Protection.** MP-7 becomes a DLP control here: policies preventing Protected B content from leaving the tenant to consumer OneDrive or unmanaged devices. Evidence includes DLP policy exports and incident reports showing enforcement.
- **PL — Planning.** The SSP for a tenant is often mis-scoped as 'M365 SSP' when it should be 'DEPT-M365 tenant configuration SSP'. Wording matters — the ATO decision is about *your* configuration, not about Microsoft 365 as a product.
- **RA — Risk Assessment.** Microsoft Secure Score is a useful *input* to RA-5 but is not itself evidence. Use Secure Score to prioritize, then produce configuration evidence for each control the score references.
- **SA — System and Services Acquisition.** SA-9 covers the third-party apps consented in the tenant. Maintain a register with business owner, data access scope, vendor risk assessment, and review date.
- **SC — System and Communications Protection.** Boundary protection in M365 is Conditional Access + Cross-Tenant Access Settings + Defender for Cloud Apps session control. Evidence includes the exported CA policy set, the CTAS configuration, and session policy definitions in MDA.

- **SI — System and Information Integrity.** Anti-malware for Exchange and SharePoint, Safe Attachments, Safe Links, and Zero-Hour Auto Purge are inherited from Microsoft when licensed; evidence is that they are *enabled* and *tuned*, with quarantine review discipline.
- **PT — Privacy.** Labels aligned to information categorization (Protected A, Protected B), retention labels aligned to departmental records disposition authorities, and Insider Risk Management policies calibrated to departmental privacy expectations.

10b.7 Representative SRTM rows for DEPT-M365

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
AC-2	Applicable	Shared	Entra ID access reviews quarterly for all directory roles and for SharePoint site administrators of Protected B sites	Access review completion export; ticketed remediation records
AC-6	Applicable	System	All Global Administrator, Exchange Admin, SharePoint Admin, and Compliance Admin roles are PIM-eligible, no permanent assignments	PIM eligible assignment export; activation history

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
AU-2	Applicable	Shared	Purview Audit (Premium) enabled tenant-wide; audit records retained per departmental policy	Audit configuration export; retention policy
CA-3	Applicable	System	Cross-tenant access settings and external identity policies define allowed partner tenants	CTAS export; enterprise app inventory with review dates
CM-2	Applicable	System	Tenant configuration managed via Microsoft365DSC in a version-controlled repository; drift reports weekly	Repo history; drift report
CP-9	Applicable	Shared	SharePoint retention labels and Preservation Hold used for records; third-party backup for high-sensitivity workloads	Retention configuration; backup restore test
IA-2	Applicable	System	Phishing-resistant MFA required for all users via Conditional Access; legacy authentication blocked	CA policy export; sign-in logs

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
MP-7	Applicable	System	DLP policies prevent Protected B content leaving the tenant to consumer endpoints	Policy exports; DLP incident sample
SC-7	Applicable	System	Boundary defined by CA + CTAS + Defender for Cloud Apps session policies	Policy exports
SI-4	Applicable	Shared	Defender XDR incidents monitored by SecOps; playbooks feed the departmental CSIRT	Incident sample with disposition
PT (Privacy)	Applicable	Shared	Sensitivity and retention labels aligned to information categorization; Insider Risk Management policies tuned to privacy expectations	Label taxonomy; IRM policy export; Privacy Office sign-off

10b.8 Assessor traps in an M365 tenant

- **'Best practice' benchmarks are not the standard.** The standard is the applicable ITSP.10.033 control set and departmental parameterization. Microsoft Secure Score and CIS M365 benchmarks are *inputs*, not the exit criteria.

- **A screenshot of one admin center blade proves one setting at one time.** Configuration exports (PowerShell, Graph, DSC) are stronger evidence.
- **License stack matters.** Some controls (e.g., Insider Risk Management, Communication Compliance) require specific license tiers. Confirm the license state before accepting configuration evidence.

Chapter 10c — Worked Example: A Protected B AI Assistant on Azure

The third worked example addresses a system class that departments are increasingly asked to authorize: a **generative AI assistant** used by public servants to search, summarize, and draft against departmental Protected B content. We will call it **'DEPT-AIA'**. It is deliberately narrower than an enterprise AI platform — one system, one categorization decision — but the guidance scales.

Because ITSP.10.033 integrates security *and* privacy controls in one catalogue, and because AI systems raise obligations under the Directive on Automated Decision-Making and the emerging Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems, AI SA&A pulls in additional governance artifacts beyond a typical Protected B web application. ISO/IEC 42001 provides a natural management-system reference for departments that want to align AI governance with an established standard (ISO 42001).

10c.1 The system

- **Name.** DEPT AI Assistant ('DEPT-AIA').
- **Purpose.** A retrieval-augmented generation (RAG) assistant that answers officer questions from a curated corpus of departmental documents and case notes, drafts routine correspondence, and summarizes long documents. It does not make decisions about citizens; it assists officers who make decisions.
- **Users.** ~2,000 officers.
- **Categorization.** Protected B / Medium integrity / Medium availability. Personal information is present in the corpus;

classification of AI *outputs* inherits the highest classification of any retrieved source.

- **ADM classification.** Under the Directive on Automated Decision-Making, DEPT-AIA is assessed via the Algorithmic Impact Assessment (AIA); at the categorization stage the system is characterized as an *assistive* rather than *automated decision* system, though the ADM classification (Level I–IV) is recorded and drives additional requirements.

10c.2 Architecture summary

- **Model layer.** Azure OpenAI Service (Canada region) with data residency committed; a base LLM plus an embedding model. No fine-tuning on departmental data in the initial release.
- **Retrieval layer.** Azure AI Search (private endpoints), semantic + vector search, indexes populated from the curated corpus.
- **Orchestration.** Azure Container Apps hosting the RAG orchestrator; prompt templates and guardrails maintained in a versioned repository.
- **Corpus and ingestion pipeline.** Azure Data Factory pulls approved documents from SharePoint Online sites into an Azure Storage account behind private endpoint, chunks and embeds them, and writes to Azure AI Search. Source documents retain their access controls; retrieval applies user-scoped filters.
- **Interface.** Web front end integrated with Entra ID SSO; per-request user identity flows to the orchestrator and is used to filter retrieval and to log actions.
- **Safety and observability.** Azure AI Content Safety filters, prompt-injection detection, output logging (with redaction), model telemetry, Microsoft Sentinel integration.
- **Human-in-the-loop.** Every output includes source citations and a persistent disclaimer; officers must review AI outputs before use.

10c.3 Authorization boundary

In boundary:

- The Azure subscription hosting DEPT-AIA (model deployments, AI Search, Container Apps, Storage, Key Vault, Log Analytics).
- The DEPT-AIA project's Azure DevOps or GitHub environment used for pipeline definitions and prompt templates.
- The ingestion pipeline components (Data Factory, staging Storage) that materialize retrieval data.
- The Entra ID Conditional Access policies scoped to DEPT-AIA.

Inherited (common service):

- Azure platform controls under CCCS Medium.
- Departmental Entra ID tenant controls (from DEPT-M365).
- Source SharePoint site controls (from DEPT-M365) — the SA&A explicitly relies on the M365 authorization.

Out of boundary:

- The public-web version of the same base model; departmental users must not use it for Protected B content.
- Consumer AI chat tools; blocked by DLP and DNS.

10c.4 What is different about SA&A for AI

Six things stretch the standard SA&A pattern:

1 **The training/tuning question.** The department must be able to state, on record, whether departmental data leaves the tenancy or is used to train shared models. For Azure OpenAI in the Canada region without fine-tuning, Microsoft's documented commitments apply; capture them in the SSP as inherited controls with references, not as verbal assurances.

2. **Prompt injection and content safety.** These are novel threats. Assurance activities under SI-3 (Malicious Code), SI-4 (System Monitoring), and SI-10 (Input Validation) extend to prompt injection defences, output filters, and adversarial testing.
3. **Retrieval scoping and 'oversharing'.** RAG systems can leak content that a user was not authorized to see if retrieval is not user-scoped. This is an AC-3 and AC-6 problem re-expressed at the retrieval layer.
4. **Output classification and downstream handling.** AI outputs inherit the highest classification of retrieved sources. This must be enforced in the UI (banners, labels) and by user training.
5. **Explainability and auditability of interactions.** Each interaction must be logged with the user, the prompt, the retrieved sources, the model version, and the response. AU-2, AU-3, AU-9 apply, with a privacy overlay.
6. **Human oversight.** The AIA and the Directive on Automated Decision-Making require documented human oversight commensurate with the ADM level. Evidence includes UI features (source citations, disclaimers), training records, and sampled audits of officer decisions that used AI assistance.

10c.5 Additional governance artifacts (beyond a typical SA&A package)

- **Algorithmic Impact Assessment (AIA)** completed and published per the TBS directive.
- **AI use-case brief / statement of intended use** describing what the system will and will not be used for; sign-off by the business owner.
- **Data lineage documentation** for the corpus: source system, extraction rules, refresh cadence, retention.
- **Prompt and guardrail change log** maintained under change control (CM-3).

- **Model card / system card** documenting the base model, version, evaluated capabilities and limitations, known failure modes, and monitoring thresholds.
- **Red-team / evaluation report** covering prompt injection, jailbreaks, sensitive information disclosure, hallucination on departmental content, and bias probes relevant to the use case.
- **User acknowledgement of AI use** — an updated PL-4 (Rules of Behavior) that specifically addresses AI use.
- **Deprovisioning / model change plan** — how the department responds when the underlying model is deprecated or upgraded.

10c.6 Representative SRTM rows unique to DEPT-AIA

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
AC-3 (retrieval)	Applicable	System	Retrieval queries include the calling user's identity; index filters restrict candidate documents to those the user is authorized to see in the source system	Orchestrator code review; end-to-end retrieval test with two users of different access
AC-6	Applicable	System	Ingestion service uses a dedicated managed identity with read-only scope; no broad service accounts	Managed identity assignment export; role scope

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
AU-2 / AU-3	Applicable	System	Every interaction logs user, prompt, retrieved source IDs, model + version, output, safety verdicts; PII redaction on stored prompts	Log schema; sample log with all fields
AU-9	Applicable	System	Interaction logs stored in immutable storage; access via privileged review workflow	Immutability policy; access review record
CM-3	Applicable	System	Prompt templates and guardrails under version control; changes reviewed and approved before deployment	PR history with approvers
RA-3 (model risk)	Applicable	System	TRA extended to cover prompt injection, data poisoning, model deprecation, and output misuse; refreshed on major model change	Signed TRA addendum
RA-5 (evaluation)	Applicable	System	Adversarial evaluation and content safety benchmarks run pre-release and on model upgrade	Eval report; regression baseline

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
SA-9 (model service)	Applicable	Shared	Azure OpenAI (Canada region) used under documented commitments regarding data residency and non-use for model training	Microsoft product documentation and contractual reference in SSP
SC-7	Applicable	System	Model, retrieval, and storage endpoints on private endpoints; egress via departmental firewall	Effective network configuration export
SI-3 (prompt injection)	Applicable	System	Input classifiers, retrieval sanitization, output filters; blocklist of known injection patterns maintained	Configuration exports; test cases
SI-4 (AI-specific)	Applicable	System	Detection rules for anomalous prompt patterns, retrieval scope escalations, sudden shifts in model behaviour	Sentinel rule set; incident samples
SI-10	Applicable	System	Prompts and retrieval snippets sanitized before insertion into model calls	Code review; test cases

Control	Applicability	Responsibility	Implementation statement (extract)	Evidence pointer
PT (Privacy)	Applicable	Shared	AIA completed; PIA updated; per-user consent to AI processing recorded where required; DPIA-equivalent for personal-information corpora	AIA record; updated PIA; consent register
PL-4 (AI use)	Applicable	System	AI-specific rules of behaviour issued and acknowledged; training completed by all users	Acknowledgement record; LMS export

10c.7 Evidence quality — AI additions

- An evaluation report that reports only average scores without adversarial coverage is not evidence for RA-5 or SI-3. Expect test-set descriptions, prompt-injection categories, refusal rates, and residual-risk narrative.
- 'Guardrails are configured' is not evidence. Guardrail *rules and thresholds*, sample outputs pre- and post-guardrail, and monitoring for guardrail bypass are.
- A model card without version pinning is not evidence — model behaviour changes with version, and the SAR should name the exact version the assessment covered.
- Human-oversight claims without sampled audits are not evidence.

10c.8 DSO decision framing for an AI system

When a DSO signs the ATO for DEPT-AIA, add three AI-specific tests to the standard reasoning in Chapter 9:

1. **Is the intended use documented and bounded?** A generative system without a bounded intended use is uncontrollable; a bounded scope keeps the risk conversation concrete.
2. **Is the human-oversight model credible?** Are officers actually reviewing outputs, or is 'human-in-the-loop' a policy fiction? Sampled evidence should exist within 90 days of go-live.
3. **Is there a re-authorization trigger for model change?** Major model version upgrades change the risk surface; the ATO letter should require re-assessment on defined trigger events, not only on the triennial cycle.

Chapter 11 — Control Family Walkthrough with Azure Evidence Expectations

This chapter walks through each ITSG-33 / ITSP.10.033 control family, using DCMS to illustrate. Under each family the tables list common evidence, what is *acceptable* to a professional assessor, and what is *not* acceptable — grounded in the assurance activities that ship with each control (ITSP.10.033).

Notational conventions:

- Control IDs use the NIST-style two-letter families (AC, AU, CM, ...) preserved by both ITSG-33 Annex 3A and ITSP.10.033.
- "Common" means inherited from Microsoft under CCCS Medium; "Shared" means partial inheritance; "System" means fully the department's.

11.1 Access Control (AC)

Objective: only authorized identities can perform authorized actions on DCMS resources and data.

Representative controls: AC-2 (Account Management), AC-3 (Access Enforcement), AC-5 (Separation of Duties), AC-6 (Least Privilege), AC-7 (Unsuccessful Logon Attempts), AC-17 (Remote Access), AC-19 (Access Control for Mobile Devices).

Control	Azure implementation	Acceptable evidence	Not acceptable
AC-2	Entra ID groups fed by HR; PIM for privileged roles; quarterly access review via Entra ID Access Reviews	Export of Access Review completion report; screenshot with reviewer name, date, decisions	Statement that "reviews happen" with no export
AC-3	Azure RBAC role assignments scoped to DCMS resource groups	RBAC assignment export (`az role assignment list`) with query and timestamp	Screenshot of one blade at one point in time
AC-5	Break-glass account separate from daily admin; deployment pipeline separates build/approve/deploy	Pipeline definition YAML with approval gates; break-glass account MFA and audit configuration	"The team follows separation of duties"
AC-6	PIM eligible assignments; Just-in-Time elevation with justification	PIM activation history export	Standing owner rights on subscription
AC-7	Entra ID smart lockout; Conditional Access policy	Policy JSON export and screenshot of enforcement in report-only test	Vendor documentation only
AC-17	Access via VPN + Conditional Access requiring compliant device	CA policy export; VPN posture check evidence	"We use VPN"

Assessor stance: for AC-2, insist on evidence that the review *decisions* were acted on (removed accounts), not just that reviews ran.

11.2 Awareness and Training (AT)

Representative controls: AT-2 (Awareness Training), AT-3 (Role-Based Training).

Control	Implementation	Acceptable evidence	Not acceptable
AT-2	Departmental annual security awareness course	LMS completion export scoped to DCMS users with dates	Aggregate corporate completion rate
AT-3	Role-based training for developers (secure coding), operators (Azure security), privileged users (PIM/PAM)	Course completions matched to named roles; agenda showing coverage	"Team attended a session"

11.3 Audit and Accountability (AU)

Representative controls: AU-2, AU-3, AU-6, AU-9, AU-11, AU-12.

Control	Azure implementation	Acceptable evidence	Not acceptable
AU-2	Diagnostic settings send platform logs to Log Analytics; Azure SQL auditing to storage + LA	Diagnostic settings export per resource; Azure Policy compliance report proving 100% coverage	Sample screenshot for one resource
AU-3	Event schema includes user, source IP, resource, action, time	Log query returning a representative record with all fields	Vendor doc only
AU-6	Sentinel analytic rules; SIEM forwarding	Rule export; incident samples with disposition	"We monitor logs"

Control	Azure implementation	Acceptable evidence	Not acceptable
AU-9	Log Analytics workspace immutable; RBAC restricts read; storage account with legal hold	Immutability policy export; RBAC list	Assurance without policy proof
AU-11	Retention set per departmental policy; archival to storage tier	Retention configuration export	Verbal statement
AU-12	Every in-scope resource emits audit events	Coverage report from Azure Policy initiative	Policy exists but not evaluated

Assessor stance: coverage is measured by Azure Policy compliance state, not by hoping.

11.4 Assessment, Authorization, and Monitoring (CA)

Representative controls: CA-2 (Control Assessments), CA-3 (Interconnections), CA-5 (PoA&M), CA-6 (Authorization), CA-7 (Continuous Monitoring), CA-9 (Internal System Connections).

Control	Implementation	Acceptable evidence	Not acceptable
CA-2	This SA&A engagement	SAP, SAR	Prior SAR only
CA-3	ISAs / MOUs with SSC and any external integration	Signed agreements; interconnection diagram	Verbal arrangement
CA-5	PoA&M as per Chapter 8	Current PoA&M with named owners	Empty PoA&M template
CA-6	ATO letter	Signed letter with scope and expiry	Draft
CA-7	ConMon plan with metrics and cadence	Plan + last quarter's ConMon report	Plan only

Control	Implementation	Acceptable evidence	Not acceptable
CA-9	Internal system connections catalogued	System connection register	Architecture diagram only

11.5 Configuration Management (CM)

Representative controls: CM-2 (Baseline), CM-3 (Change Control), CM-6 (Configuration Settings), CM-7 (Least Functionality), CM-8 (Inventory), CM-10, CM-11.

Control	Azure implementation	Acceptable evidence	Not acceptable
CM-2	Infrastructure as Code (Bicep/Terraform); Azure Policy for platform baseline	Repo history; policy definitions and compliance state	Manual portal changes
CM-3	Change advisory board; PR reviews with approvers; Change tickets	Ticket export with approvers; PR history	"Changes are reviewed"
CM-6	Azure Policy `deployIfNotExists` for hardening	Policy compliance report; guest configuration reports for VMs	Baseline document with no enf orcement
CM-7	Only required ports open; Front Door / WAF rules	Effective NSG/route table export; WAF ruleset version	Design doc only

Control	Azure implementation	Acceptable evidence	Not acceptable
CM-8	Azure Resource Graph inventory	Resource Graph query with timestamp	Old CMDB export

11.6 Contingency Planning (CP)

Representative controls: CP-2 (Contingency Plan), CP-4 (Testing), CP-9 (Backups), CP-10 (Recovery).

Control	Azure implementation	Acceptable evidence	Not acceptable
CP-2	DR plan aligned to RTO/RPO	Signed plan with roles and criteria	Plan >12 months old
CP-4	Annual DR test	Test plan, results, lessons learned	"DR tested" without artifacts
CP-9	Azure Backup with geo-redundancy; SQL PITR	Backup policy export; restore test log	Backup policy exists, no restore test
CP-10	Documented recovery runbooks	Runbook + evidence of run in test	Runbook without test

11.7 Identification and Authentication (IA)

Representative controls: IA-2 (User Identification and Authentication), IA-4 (Identifier Management), IA-5 (Authenticator Management), IA-8, IA-12.

Control	Azure implementation	Acceptable evidence	Not acceptable
IA-2	Entra ID with phishing-resistant MFA (FIDO2 / Windows Hello for Business) for all users; certificate-based for privileged	Conditional Access policy export; sign-in logs showing MFA method distribution	"MFA is enforced"
IA-5	Password + authenticator policy; secrets managed in Key Vault; managed identities for workloads	Entra ID authentication methods policy; Key Vault access review; enumeration proving no static secrets in code	Grep of one repo
IA-8	Federation with SSC / partner identity where applicable	Federation configuration; sign-in logs	Verbal

11.8 Incident Response (IR)

Representative controls: IR-2, IR-4, IR-6, IR-8.

Control	Implementation	Acceptable evidence	Not acceptable
IR-4	Sentinel playbooks; departmental CSIRT integration	Playbook definitions; recent tabletop after-action report	Playbook only
IR-6	Notification to departmental CSIRT and to CCCS as required	Notification records for a prior incident (redacted if needed)	"We would notify"
IR-8	Documented IR plan with roles	Plan + last exercise report	Plan only

11.9 Maintenance (MA)

Most maintenance controls in a fully cloud-native system are inherited from Microsoft. Acceptable evidence is the CCCS Medium attestation. The department retains responsibility for maintenance of guest OS in containers and any customer-managed VMs.

11.10 Media Protection (MP)

Representative controls: MP-2, MP-4, MP-5, MP-6, MP-7.

For a cloud-native system, MP is largely inherited from Microsoft (secure disposal of storage media). Where the department downloads Protected B data to endpoints, MP-7 (Media Use) and DLP configurations are the department's responsibility. Acceptable evidence includes Purview DLP policies and endpoint policies preventing removable storage.

11.11 Physical and Environmental Protection (PE)

Fully inherited from Microsoft under CCCS Medium at Protected B. Acceptable evidence is Microsoft's attestation (CCCS Medium). Not acceptable: hand-waving without pointing at the specific inherited controls.

11.12 Planning (PL)

Representative controls: PL-2 (System Security Plan), PL-4 (Rules of Behavior), PL-8 (Security Architecture).

The SSP itself is evidence for PL-2. Rules of Behavior (PL-4) evidence is the departmental acceptable-use policy and the record of user acknowledgement. PL-8 evidence is the security architecture document and its formal review.

11.13 Personnel Security (PS)

Personnel screening is a departmental function performed to the levels required by the Standard on Security Screening. Acceptable evidence is screening completion records at the appropriate level (Reliability, Secret, etc.) for all users of DCMS. Not acceptable: a signed attestation without back-up records.

11.14 Risk Assessment (RA)

Representative controls: RA-3 (Risk Assessment), RA-5 (Vulnerability Monitoring and Scanning), RA-7 (Risk Response).

Control	Azure implementation	Acceptable evidence	Not acceptable
RA-3	TRA using the Harmonized TRA methodology	Signed TRA with threat-actor analysis	Generic risk register
RA-5	Defender for Cloud CSPM + CWPP; container scanning in pipeline; DAST	Vulnerability report with severity, first-seen, target dates; ticket linkage	Point-in-time dashboard screenshot
RA-7	Vulnerability SLAs by severity	Aging report with adherence percentage	"We fix them quickly"

11.15 System and Services Acquisition (SA)

Representative controls: SA-4 (Acquisition Process), SA-9 (External System Services), SA-11 (Developer Testing), SA-15 (Development Process).

Control	Implementation	Acceptable evidence	Not acceptable
SA-4	Security requirements included in procurement	RFP language; SLAs	Vendor claim
SA-9	External services (CSPs, SaaS) authorized or assessed	Inherited authorization letters; vendor risk assessments	"We use vendor X"
SA-11	SAST, SCA, DAST in pipeline	Pipeline logs; last release scan reports	Tool exists but not used
SA-15	Secure SDLC	SDLC document; secure design review notes	Verbal

11.16 System and Communications Protection (SC)

Representative controls: SC-7 (Boundary Protection), SC-8 (Transmission), SC-12/13 (Cryptographic Key Management), SC-23 (Session Authenticity), SC-28 (Protection at Rest).

Control	Azure implementation	Acceptable evidence	Not acceptable
SC-7	Front Door + WAF; NSGs; Azure Firewall; private endpoints	Effective ruleset exports; policy compliance	Diagram only
SC-8	TLS 1.2+ enforced; mutual TLS on internal service traffic	TLS configuration export; scan result (e.g., Qualys SSL Labs)	"We use HTTPS"

Control	Azure implementation	Acceptable evidence	Not acceptable
SC-12/13	Key Vault HSM (FIPS 140-2 Level 2/3); CMK for SQL, Storage; rotation	Key Vault configuration; rotation history; FIPS references from Microsoft	CSP marketing page only
SC-23	Cookie flags, anti-CSRF, session timeout	Configuration proof; DAST evidence	Code comment
SC-28	TDE + CMK; Storage encryption with CMK	Configuration export	Statement

11.17 System and Information Integrity (SI)

Representative controls: SI-2 (Flaw Remediation), SI-3 (Malicious Code), SI-4 (System Monitoring), SI-7 (Software Integrity), SI-10 (Input Validation), SI-11 (Error Handling).

Control	Azure implementation	Acceptable evidence	Not acceptable
SI-2	Patch pipeline; container base image rebuilds; SLAs	Adherence report; sample tickets	Ad-hoc
SI-3	Defender for Cloud; endpoint EDR	Coverage report	Purchase order
SI-4	Sentinel + custom analytics; anomaly detection	Rule set; sample alerts	Product name only
SI-7	Signed containers; supply chain attestation (SBOM, provenance)	SBOM export; signature verification logs	"We build securely"
SI-10	Input validation library; server-side validation confirmed	Code review notes; DAST evidence	Framework claim

11.18 Privacy controls (PT/PA family under ITSP.10.033)

Under ITSP.10.033 the privacy family is integrated. For a Protected B system that handles personal information, at minimum expect:

- A completed PIA endorsed by the departmental privacy office.
- Records of collection, use, disclosure, retention, and disposal aligned to the Privacy Act and applicable regulations.
- Data minimization evidence — schema review showing no unnecessary personal information.
- Privacy notices to end users where applicable.

Chapter 12 — Continuous Authorization, Reassessment, and Change Management

The ATO is not the end. Continuous monitoring — anchored by control CA-7 — is where authorization stays honest.

12.1 A workable ConMon rhythm

Cadence	Activity
Continuous	Sentinel alerts; Defender for Cloud posture score; Policy compliance
Monthly	Vulnerability aging; access review deltas; PoA&M status
Quarterly	Sample control re-test; access certifications; DR component test
Annual	Full DR test; TRA refresh; SSP delta; ATO health check
Triennial	Full reassessment and ATO renewal

12.2 Change management and re-authorization triggers

Trigger a delta assessment when:

- Boundary changes materially (new subscription, new tenant, new external integration).
- Categorization changes (new data class ingested).
- A high-impact finding is opened or a security incident of significance occurs.

- Common-service posture changes (e.g., Microsoft's CCCS Medium status changes, or SSC changes a transit service).

12.3 Continuous ATO patterns

Some departments move toward "continuous authorization" — the ATO remains valid as long as ConMon evidence remains within thresholds. Two prerequisites make this workable: (1) machine-readable evidence pipelines (Azure Policy compliance, Defender for Cloud secure score, Sentinel incident MTTR) feeding a ConMon dashboard; and (2) explicit thresholds in the ATO letter that, if breached, revert the system to interim status.

Chapter 13 — Bridging from ISO 27001, NIST 800-53/800-37, FedRAMP, and SOC 2

13.1 If you come from ISO 27001

- Your **ISMS scope** is a boundary — but the GC boundary is *system-specific*, not organization-wide. Expect to draw a narrower line.
- Your **Statement of Applicability** maps to the SRTM. GC applicability decisions are per control *with parameterization*; ISO 27001 A-controls are lighter. Expect more work.
- Your **management reviews and internal audits** correspond to the DSO's risk oversight and to CA-7 continuous monitoring — but the GC expects specific control-level assurance, not just management review outputs.
- Your **certification body** does not exist in GC SA&A. The DSO is the authorizer; there is no third-party certification stamp.
- The good news: ISO 27001 clause 6 risk assessment and Annex A operating discipline transfer directly. Where your SoA justifies "not applicable" with reference to the risk assessment, replicate the same discipline in the SRTM.

13.2 If you come from NIST 800-53 and 800-37

- You already know the control families and the RMF. ITSP.10.033 preserves both — the Foreword explicitly aligns with the US

baseline to support common risk management (ITSP.10.033 Foreword).

- Terminology mapping: Authorizing Official → DSO; System Owner → System / Project Authority; ISSO → security practitioner; POA&M → PoA&M; SSP/SAP/SAR/POA&M package → same, plus a Statement of Sensitivity.
- Watch for: GC categorization uses *Protected A/B/C* (confidentiality) and *Low/Medium/High* injury for integrity and availability, not FIPS 199 impact levels. Do not blindly translate "Moderate" to "PBMM"; verify against injury.

13.3 If you come from FedRAMP

- The FedRAMP SSP, SAP, SAR, SRTM, and POA&M templates transfer with light editing. GC does not run a central marketplace equivalent to the FedRAMP Marketplace; CCCS runs the CSP assessment program upstream, and each department authorizes its own use.
- Continuous monitoring artifacts (monthly ConMon deliverables) map directly to the GC ConMon rhythm.
- Independent 3PAO discipline maps to GC independent assessors; the profession is smaller but the expectations are the same.

13.4 If you come from SOC 2

- SOC 2 evidence quality is close to what a GC assessor expects: sampled, reproducible, timeboxed. Reuse population + sample discipline.
- SOC 2 report reuse: a Type II report can *inform* inheritance and vendor-risk decisions but does not substitute for GC assessment of the customer-managed layer. Where the CSP has a CCCS letter, the CCCS letter is the primary reliance document (ITSP.50.105 notes that FedRAMP, SOC, ISO, and CSA STAR can *supplement* CSP-level assurance).
- Exceptions in SOC 2 Section 4 map to PoA&M items — the same discipline of evidence, disposition, and remediation applies.

Chapter 14 — Training, Certifications, and How to Break Into GC SA&A Work

14.1 Foundational learning

- Read the primary sources first, in this order: TBS Policy on Government Security → Directive on Security Management → ITSG-33 Overview → ITSG-33 Annex 2 → ITSG-33 Annex 3A → ITSP.10.033 → ITSP.50.105.
- Take the CCCS Learning Hub courses, especially Cloud computing in the GC — The security assessment and authorization process (CLD201C).
- Read NIST SP 800-37 Rev. 2 and NIST SP 800-53A cover to cover once — they are the ancestors of everything you will do in Canada.

14.2 Certifications that transfer well

For practitioners and assessors moving into GC SA&A, the most useful credentials are those that reinforce the same discipline:

- **ISC² CGRC** (formerly CAP) — the closest single-exam credential to the RMF/SA&A workflow.
- **ISACA CISA** — for assessment discipline, evidence, and sampling.
- **ISACA CRISC** — for the risk-management lens.
- **ISO/IEC 27001 Lead Implementer and Lead Auditor (PECB / BSI)** — implementation and evidence rigor that transfers directly.
- **ISO/IEC 42001 Lead Implementer** — as ITSP.10.033 folds privacy in and departments begin adding AI systems, this credential positions you well.

- **CISSP** — broad breadth remains a common departmental preference for senior roles.
- **Cloud provider credentials** — for Azure work, at minimum the Microsoft SC-100 (Cybersecurity Architect Expert) and AZ-500 (Azure Security Engineer); for AWS work, AWS Certified Security — Specialty.

14.3 What a hiring manager or contracting authority actually looks for

For an assessor engagement:

- Prior SA&A engagements you can describe (redacted) — boundary, categorization, deliverables, findings, disposition.
- Evidence of independence and professional interpretation — not just tool operation.
- Familiarity with the specific hosting environment (Azure, AWS, GCP, SSC on-prem).
- Working knowledge of the ITSG-33 → ITSP.10.033 transition (this book).

For a practitioner engagement:

- Ability to write an SSP that is defensible, not just complete.
- Ability to build an SRTM and manage tailoring conversations with architects and business owners.
- Comfort with the departmental risk conversation, including compensating controls and PoA&M discipline.

14.4 A 90-day transition plan for a private-sector professional

Weeks 1–2. Read the primary sources listed above. Skim ITSP.10.033 in full; do not memorize.

Weeks 3–4. Take one CCCS learning-hub course and one Azure security course (SC-100 or AZ-500 study material).

Weeks 5–6. Rebuild a familiar system (from prior ISO 27001 / SOC 2 / FedRAMP work) as if it were a GC Protected B system. Draft: SoS, boundary diagram, SRTM against the ITSP.10.033 medium profile, an SSP outline, and a PoA&M with five illustrative findings.

Weeks 7–8. Have a peer or mentor with GC experience review the artifacts and give red-ink feedback. Iterate.

Weeks 9–10. Study for and sit CGRC or ISO 27001 Lead Implementer if you do not already hold an equivalent credential.

Weeks 11–12. Apply — to a systems integrator's GC practice, a boutique GRC firm, a departmental contract vehicle (SBIPS, TBIPS, ProServices), or directly to a hiring department. Bring the rebuilt artifacts as a portfolio.

Appendix A — Deliverables Matrix (RACI)

R = Responsible, A = Accountable, C = Consulted, I = Informed.

Deliverable	Business Owner	System Owner	Practitioner	Assessor	Privacy	DSO
Statement of Sensitivity	A	C	R	I	C	I
Threat & Risk Assessment	C	A	R	C	C	I
Privacy Impact Assessment	C	A	C	I	R	I
SRTM	I	A	R	C	C	I
System Security Plan	C	A	R	C	C	I
Security Assessment Plan	I	C	C	R	I	A
Security Assessment Report	I	C	C	R	I	A
PoA&M	I	A	R	C	C	I
ATO letter	I	C	C	C	C	R/A

Deliverable	Business Owner	System Owner	Practitioner	Assessor	Privacy	DSO
ConMon reports	I	A	R	C	I	I

Appendix B — Evidence Quality Rubric

Dimension	Score 3 (Strong)	Score 2 (Adequate)	Score 1 (Weak)	Score 0 (Reject)
Authenticity	Signed export, tool chrome and metadata visible	Screenshot with clear source	Screenshot only	Verbal statement
Contemporaneity	Within assessment window	Within 90 days	Within 12 months	Older than 12 months
Completeness	Full population	Statistically sampled	Judgemental sample	Single instance
Reproducibility	Query and parameters recorded	Query recorded	Method recorded	Not reproducible

Findings should record the dimension scores. Evidence with a 0 on any dimension is not evidence.

Appendix C — PoA&M Risk Scoring

Use a 5×5 likelihood/impact heat map. Impact uses injury language consistent with the SoS (Injury to Canadians, to the Crown, to the department, financial). Likelihood uses threat-actor motivation and opportunity language from the Harmonized TRA methodology. Score each PoA&M item at *inherent* and *residual* levels; the residual score drives DSO acceptance decisions.

Appendix D — Glossary

- **ATO** — Authority to Operate.
- **CCCS** — Canadian Centre for Cyber Security.
- **ConMon** — Continuous monitoring.
- **DSO** — Departmental Security Officer.
- **IATO** — Interim Authority to Operate.
- **ISSIP** — Information System Security Implementation Process (ITSG-33 Annex 2).
- **PBMM** — Protected B / Medium integrity / Medium availability.
- **PIA** — Privacy Impact Assessment.
- **PoA&M** — Plan of Action and Milestones.
- **SA&A** — Security Assessment and Authorization.
- **SAP** — Security Assessment Plan.
- **SAR** — Security Assessment Report.
- **SoS** — Statement of Sensitivity.
- **SRTM** — Security Requirements Traceability Matrix.
- **SSC** — Shared Services Canada.
- **TRA** — Threat and Risk Assessment.

Appendix E — Source Register

Primary Government of Canada references:

- Policy on Government Security (TBS)
- Directive on Security Management (TBS)
- ITSG-33 — IT Security Risk Management: A Lifecycle Approach (CCCS)
- ITSG-33 Annex 2 — Information system security risk management activities
- ITSG-33 Annex 3A — Security control catalogue
- ITSG-33 Annex 4A Profile 1 — PBMM (PDF)
- ITSP.10.033 — Security and privacy controls and assurance activities catalogue
- ITSP.10.033 Foreword, Overview, Introduction
- ITSP.10.033 (full PDF)
- ITSP.10.033-01 medium-impact profile
- ITSP.50.105 — Guidance on cloud security assessment and authorization
- ITSM.50.100 — CSP IT Security Assessment Process
- ITSM.50.109 — Manage GC Data in Cloud (PDF)
- GC Security Control Profile for Cloud-Based IT Services
- GC Cloud Security Risk Management Approach and Procedures
- Harmonized TRA methodology
- Standard on Security Screening (TBS)
- Privacy Act
- SSC Audit of Security Assessment and Authorization (2020)

US references used for concepts, terminology, and template shapes:

- NIST SP 800-37 Rev. 2 — Risk Management Framework
- NIST glossary — authorization boundary
- FedRAMP SAR template-Template.docx)
- FedRAMP High SRTM template
- FedRAMP Moderate SRTM template
- FedRAMP Authorization Boundary Guidance
- FedRAMP System Security Plan template.docx)

Cloud provider assessment references:

- Microsoft — CCCS Medium offering
- Microsoft — Canada Protected B offering

End of book.