eBOOK · ITSG-33

ITSG-33 SA&A; Demystified: A Vendor's Guide to Canadian Government Compliance

Break down the Security Assessment & Authorization process — control profiles, evidence requirements, and how to accelerate your departmental approval.

44 pages · PDF · Updated May 2026 · **goironfort.com**

Introduction

ITSG-33 — IT Security Guidance 33, "IT Security Risk Management: A Lifecycle Approach" — is the Canadian Centre for Cyber Security's framework for managing IT security risks within the Government of Canada. For technology vendors seeking federal or provincial government contracts, ITSG-33 compliance and a valid Authorization to Operate (ATO) are not optional: they are prerequisites.

Unlike SOC 2 or HIPAA, ITSG-33 is not well-documented outside of government circles. This guide translates the framework into plain language for technology vendors navigating it for the first time.

Understanding the SA&A; Lifecycle

The Security Assessment and Authorization (SA&A;) process is the GC's formal mechanism for authorizing systems to operate within government environments. It has six phases:

Phase 1: Initiation

Define system boundaries, roles, and the SA&A; plan. Assign an Authorizing Official (AO), SA&A; Coordinator, and System Owner.

Phase 2: System Description

Document the system in System Security Plan (SSP) format — architecture, data flows, interconnections, classification levels.

Phase 3: Control Selection

Select the ITSG-33 security control profile appropriate to your data classification (Unclassified / Protected A / Protected B). Document implementation statements for each applicable control.

Phase 4: Security Assessment

A third-party Security Assessment Service Provider (SASP) assesses your control implementations. Findings are documented in a Security Assessment Report (SAR).

Phase 5: Authorization

Compile the Authorization Package for the AO: SSP, SAR, Plan of Action & Milestones (PoA&M;), and residual risk acceptance documentation.

Phase 6: Continuous Monitoring

Ongoing control monitoring, annual security reviews, and change management impact assessments.

Data Classification Levels

Classification	Control Count	ITSG-33 Profile	Example Data Types
Unclassified	~80 controls	Low profile	Public information, non-sensitive administrative data
Protected A	~200 controls	Medium profile	Sensitive personal information (name + address, employee records)
Protected B	330+ controls	High profile	Highly sensitive data: SIN, tax records, health information, biometrics

ITSG-33 Control Families

ITSG-33 Annex 3 security controls are organized into 18 families, mirroring NIST SP 800-53. Each family contains baseline controls applicable across classification levels, plus enhancements required at higher sensitivity tiers.

AC — Access Control	**AT** — Awareness & Training	**AU** — Audit & Accountability
CA — Security Assessment	**CM** — Configuration Mgmt	**CP** — Contingency Planning
IA — Identification & Auth	**IR** — Incident Response	**MA** — Maintenance
MP — Media Protection	**PE** — Physical & Env.	**PL** — Planning
PS — Personnel Security	**RA** — Risk Assessment	**SA** — System & Services
SC — System & Comm.	**SI** — System & Info Integrity	**PM** — Program Mgmt

GC Cloud Guardrails

Any cloud service processing GC data must comply with SSC's 12 GC Cloud Guardrails. These are a mandatory baseline that must be validated before Protected data can be processed in the cloud.

- 1. Protect root / global admins (enforce MFA)
- 2. Manage access through identity federation

- 3. Enable multi-factor authentication
- 4. Enable logging and monitoring
- 5. Implement data protection at rest
- 6. Protect data-in-transit
- 7. Protect the management console and APIs
- 8. Segment and separate
- 9. Network security services
- 10. Establish cyber defence services
- 11. Enable alerting for the GC
- 12. Configuration of cloud marketplaces

Get Your Free SA&A; Readiness Assessment

Iron Fort automates the ITSG-33 SA&A; lifecycle — from control profile mapping through Authorization Package generation. Book a free readiness assessment at **goironfort.com/demo** — we'll review your target contract and map your fastest path to ATO.