SmartSuite

Framework / Cloud Security / Other

Cloud Security Assessment and Authorization Guidance (CSAG)

Canada CSAG guides Canadian public sector organizations in assessing, authorizing, and managing cloud service security to meet regulatory requirements.

What it is

Canada CSAG (Cloud Security Assessment and Authorization Guidance) is a cybersecurity and compliance framework that helps organizations assess, authorize, and manage the security of cloud services within the Canadian public sector. Its primary purpose is to support organizations in evaluating cloud service providers against defined security requirements to ensure data protection and regulatory compliance.

The guidance is published by the Canadian Centre for Cyber Security (CCCS) and is primarily used by Canadian government departments, agencies, and cloud service providers seeking approval to handle sensitive data. CSAG covers focus areas such as risk assessment, security controls, continuous monitoring, and compliance oversight for cloud-based environments, ensuring alignment with Canadian privacy and risk management standards.

At a glance

PUBLISHER Office of the Superintendent of Financial Institutions (OSFI)	TYPE Framework	VERSION 1.0
EFFECTIVE 2022	DOMAIN Cloud Security	FAMILY Other
REGION Canada	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: https://www.osfi-bsif.gc.ca/en/risks/technology-cyber-risk-management/cyber-security-self-assessment

Why it matters

- **Strengthen cloud security governance** Enable consistent assessment and management of cloud security risks through structured evaluation and ongoing oversight processes.
- **Enhance regulatory compliance** Support alignment with Canadian privacy, risk, and data protection regulations to facilitate approval for handling sensitive government information.
- **Improve third-party risk management** Assist in systematically evaluating cloud service providers' controls, reducing the risk of data breaches and vendor-related incidents.
- **Increase audit readiness** Facilitate the preparation and documentation necessary for demonstrating due diligence to auditors, regulators, and stakeholders.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CSAG

Self-Assessment Questionnaire Structure

Run structured cyber self-assessments with scoring and evidence attachments.

Gap Remediation Roadmap

Convert findings into a prioritized roadmap with owners and milestones.

Evidence and Practice Documentation

Centralize proof that practices are defined, performed, and repeatable.

Maturity Progression Tracking

Track maturity progression over time with measurable indicators.

Governance Reporting and Reviews

Schedule periodic reviews and maintain leadership reporting evidence.

Corrective Action and Program Enhancement Tracking

Track corrective actions, closure verification, and program enhancements.

Common framework mappings

CSA STAR | FedRAMP Rev. 5 | ISO 27001:2022 | ISO 27017 | ISO 27018 | NIST 800-53 Rev.5

Official resources

Canada CSAG Overview

Provides a comprehensive guide to Canada's Cloud Security Assessment and Authorization process.

cyber.gc.ca/en/guidance/cloud-security-risk-management-itsm50062

Cyber Security Self-Assessment Guidance

Outlines self-assessment processes for Canadian cybersecurity risk management.

osfi-bsif.gc.ca/en/risks/technology-cyber-risk-management/cyber-security-self-assessment

Frequently asked questions

What is Canada CSAG used for?

Canada CSAG is used to assess, authorize, and manage the security of cloud services within the Canadian public sector. The guidance ensures that cloud service providers meet defined security requirements for protecting sensitive data and supporting regulatory compliance.

Is Canada CSAG mandatory or certifiable?

Canada CSAG is not a certifiable standard, but compliance is required for cloud service providers seeking to offer services to Canadian government organizations. Adherence to CSAG is typically mandated through procurement requirements or internal policy for handling protected and sensitive information.

What organizations are in scope for Canada CSAG?

CSAG primarily applies to Canadian federal government departments, agencies, and their third-party cloud service providers. It may also be referenced by organizations handling sensitive or regulated data under Canadian jurisdiction.

What are the key concepts and artifacts required for Canada CSAG compliance?

Key artifacts for CSAG compliance include risk assessment reports, security control mappings, system security plans, and formal authorization packages. The framework also requires evidence of continuous monitoring, control testing, and supplier assurance activities.

How does an organization implement the Canada CSAG framework?

Organizations implement CSAG by mapping their existing security controls to the CSAG control catalog, conducting risk assessments, and preparing authorization packages for cloud services. Implementation also involves establishing governance structures, assigning control ownership, and documenting compliance status.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How does Canada CSAG relate to other security frameworks?

Canada CSAG aligns with Canadian privacy and risk management standards and may harmonize with international frameworks such as NIST and ISO 27001. It builds on global best practices while addressing Canada-specific regulatory and jurisdictional requirements for data protection.

What are the ongoing compliance requirements for Canada CSAG?

Maintaining CSAG compliance requires regular continuous monitoring, periodic risk and security assessments, control testing, and evidence collection. Organizations must periodically review and update authorization packages and demonstrate remediation of identified risks.

How would SmartSuite support Canada CSAG?

SmartSuite supports Canada CSAG by enabling organizations to assign and track control ownership, link controls to risk registers, and automate evidence collection. The platform facilitates control testing, remediation tracking, audit readiness, and consolidated reporting to maintain continuous compliance and transparency for regulators and stakeholders.

License included / downloadable: Yes Canada's Cloud Security Assessment and Authorization Guidance is published by Canadian government authorities and is publicly available through official government resources.

Full framework page and mappings: smartsuite.com/frameworks/canada-csag-cloud-security-assessment-and-authorization-guidance

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.