

# CSE ITSP.10.171

ITSP.10.171 guides organizations in identifying, assessing, and managing risks from cyber security events to improve resilience.



## What it is

Canada ITSP.10.171 — Cyber Security Risk Management for Cyber Security Events is a national cybersecurity framework that assists organizations in effectively identifying, assessing, and managing risks associated with cyber security events. Its primary purpose is to strengthen cyber resilience by guiding organizations in preparing for, responding to, and recovering from security incidents.

Published by the Canadian Centre for Cyber Security (CCCS), ITSP.10.171 is intended for both public and private sector organizations operating within Canada. The framework focuses on key areas such as cyber risk management, incident response, security controls implementation, and continuous improvement in cyber security event handling, aligning with other standards like NIST and ISO for comprehensive risk oversight.

## At a glance

|                                                 |                                   |                                       |
|-------------------------------------------------|-----------------------------------|---------------------------------------|
| PUBLISHER<br>Canadian Centre for Cyber Security | TYPE<br>Framework                 | VERSION<br>ITSP.10.171                |
| EFFECTIVE<br>2019                               | DOMAIN<br>Cybersecurity           | FAMILY<br>NIST Special Publications   |
| REGION<br>Canada                                | ADOPTION MODEL<br>Risk Management | IMPLEMENTATION COMPLEXITY<br>Moderate |

Source: <https://www.cyber.gc.ca/en/guidance/protecting-specified-information-non-government-canada-systems-and-organizations-itsp10171>

## Why it matters

- **Strengthen cybersecurity governance** Support consistent, organization-wide processes for cyber risk assessment, incident response, and continuous security improvement.
- **Enhance incident response capabilities** Enable faster detection and more effective management of cybersecurity events, minimizing business impact and recovery time.
- **Promote regulatory and standards alignment** Facilitate alignment with Canadian and international cybersecurity requirements, supporting compliance and simplifying audits.
- **Improve protection of sensitive data** Implement controls and procedures that safeguard sensitive information from unauthorized access, loss, or disclosure during cyber events.

How SmartSuite supports ITSP.10.171

Cybersecurity Risk Management Framework

Structure risk management processes, policies, and control requirements aligned to ITSP guidance.

Cybersecurity Risk Assessment and Treatment

Identify, assess, and monitor cybersecurity risks across systems and operations.

Incident Detection and Response Workflows

Manage security incidents, escalation procedures, and coordinated response activities.

Security Monitoring and Event Management

Track logs, alerts, and monitoring activities to detect and analyze threats.

System Protection and Control Implementation

Manage implementation of safeguards protecting government systems and sensitive information.

ITSP Compliance Reporting

Provide dashboards showing risk posture, incident status, and ITSP compliance readiness.

Common framework mappings

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

MITRE ATT&CK

NIST CSF 2.0

NIST 800-37 Rev.2

NIST 800-53 Rev.5

Official resources

ITSP.10.171 Framework Document

Defines requirements for managing cybersecurity risks and events, published by the CCCS.

[cyber.gc.ca/en/guidance/protecting-specified-information-non-government-canada-systems-and-organizations-itsp10171](https://cyber.gc.ca/en/guidance/protecting-specified-information-non-government-canada-systems-and-organizations-itsp10171)

Frequently asked questions

What is Canada ITSP.10.171 used for?

Canada ITSP.10.171 provides organizations with a structured approach to identifying, assessing, and managing risks related to cyber security events. It guides the development of incident response, detection, and recovery processes to enhance cyber resilience.

Is Canada ITSP.10.171 mandatory or certifiable?

Canada ITSP.10.171 is not a mandatory or certifiable standard. Rather, it serves as recommended guidance from the Canadian Centre for Cyber Security (CCCS) to help organizations strengthen their cyber event risk management aligned with Canadian regulatory expectations.

Who should use Canada ITSP.10.171?

Canada ITSP.10.171 is applicable to both public and private sector organizations operating in Canada that process, store, or manage sensitive or regulated digital information, and require robust cyber event risk management.

What are the key components or artifacts required by Canada ITSP.10.171?

Key components of ITSP.10.171 include documented risk assessments for cyber events, incident response plans, event detection and reporting procedures, and evidence of ongoing control implementation and testing. Organizations are expected to maintain records for governance and audit purposes.

How does Canada ITSP.10.171 approach risk management?

The framework applies a dual-lifecycle model, integrating risk management and incident management processes. Organizations assess event-specific risks, implement preventive and detective controls, and follow defined escalation and reporting mechanisms throughout the incident lifecycle.

### **How does Canada ITSP.10.171 relate to other frameworks like NIST or ISO standards?**

Canada ITSP.10.171 aligns closely with controls and principles in widely recognized standards such as NIST and ISO/IEC 27001, particularly in incident response and risk management. This enables organizations to build a harmonized compliance posture across multiple regulatory and standards-based requirements.

### **What are the ongoing compliance requirements for Canada ITSP.10.171?**

Ongoing compliance involves regular risk reviews, periodic testing of incident response procedures, control effectiveness monitoring, continuous improvement activities, and documentation of all cyber security events and remediation actions for oversight and audit trails.

### **How would SmartSuite support Canada ITSP.10.171?**

SmartSuite streamlines ITSP.10.171 compliance by providing configurable control libraries, a centralized risk register, and incident management modules. The platform enables evidence collection, tracks implementation status, manages remediation workflows, facilitates audit readiness, and delivers dashboards for monitoring and reporting on cyber security governance and risk posture.

License included / downloadable: Yes ITSP.10.171 is published by the Canadian Centre for Cyber Security and is publicly available through official Canadian government resources.

Full framework page and mappings: [smartsuite.com/frameworks/canada-itsp-10-171-cyber-security-risk-management-for-cyber-security-events](https://smartsuite.com/frameworks/canada-itsp-10-171-cyber-security-risk-management-for-cyber-security-events)