

2 PART WEBINAR SERIES | WEBINAIRES EN DEUX PARTIES

Part 2: Understanding the Legal Framework for Digital Security and Privacy in B.C. and Building Organizational and Institutional Policies for the Settlement and Integration Sector

2^{re} partie : Comprendre le cadre juridique de la sécurité numérique et de la protection de la vie privée en Colombie-Britannique pour élaborer et mettre en place des politiques organisationnelles et institutionnelles dans le secteur de l'établissement et de l'intégration

May 14, 2024
14 mai 2024





As a provincial umbrella association, AMSSA acknowledges that B.C. is on the unceded homelands of First Nations who have stewarded this land since time immemorial. We recognize the privilege that we have as settlers on this land and acknowledge that AMSSA's operations is on the unceded traditional territories of the x^wməθkwəyəm (Musqueam), Skwxwú7mesh (Squamish), and Səlílwətaʔ/Selilwítlh (Tsleil-Waututh) Nations. As an organization, AMSSA is committed to creating a safe space for indigenous voices.

AMSSA, organisme-cadre provincial, reconnaît que la Colombie-Britannique se trouve sur les territoires non cédés des Premières nations qui habitent ces terres depuis des temps immémoriaux. Elle admet que ses activités se déroulent sur les territoires traditionnels non cédés des nations x^wməθkwəyəm (Musqueam), Skwxwú7mesh (Squamish) et Səlílwətaʔ/Selilwítlh (Tsleil-Waututh), et est reconnaissante du privilège que nous avons de travailler sur ces territoires. En tant qu'organisation, AMSSA s'engage à créer des espaces sûrs où les points de vue des Autochtones peuvent être entendus.

Funded by Financé par



Immigration, Refugees
and Citizenship Canada

Immigration, Réfugiés
et Citoyenneté Canada

Understanding the Legal Framework for Digital Security and Privacy in B.C. and Building Organizational and Institutional Policies for the Settlement and Integration Sector

Comprendre le cadre juridique de la sécurité numérique et de la protection de la vie privée en Colombie-Britannique pour élaborer et mettre en place des politiques organisationnelles et institutionnelles dans le secteur de l'établissement et de l'intégration

Speaker / Conférencier

JAMIE HARI

Canadian Internet Registration Authority (CIRA)

Cette formation est présentée par
l'Autorité canadienne pour les enregistrements
Internet (ACEI)





Information Security Webinar

Part 2



Webinaire sur la sécurité de l'information

Partie 2

Introduction to principles

Introduction aux principes

Confidentiality, Integrity, Availability



Confidentialité, Intégrité, Disponibilité



Introduction to principles

Introduction aux principes

Data security

- Data in transit
- Data at rest
- Data in use

Sécurité des données

- Données en transit
- Données au repos
- Données utilisées

Part 2

Partie 2

Topics

- Digital security and privacy: laws, regulations, and frameworks.
- Security program management: policies, incident management, and oversight.

Thèmes

- Sécurité et confidentialité numériques : lois, règlements, et cadre.
- Gestion du programme de sécurité : politiques, gestion des incidents, et surveillance.



Frameworks, Regulations, and Laws

Cadres, Règlements et Lois

Frameworks, Regulations, and Laws

Cadres, Règlements et Lois

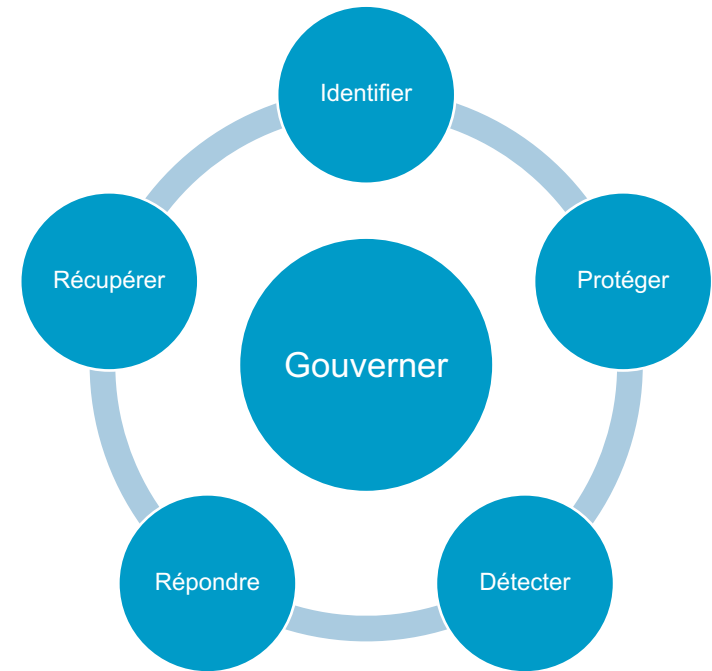
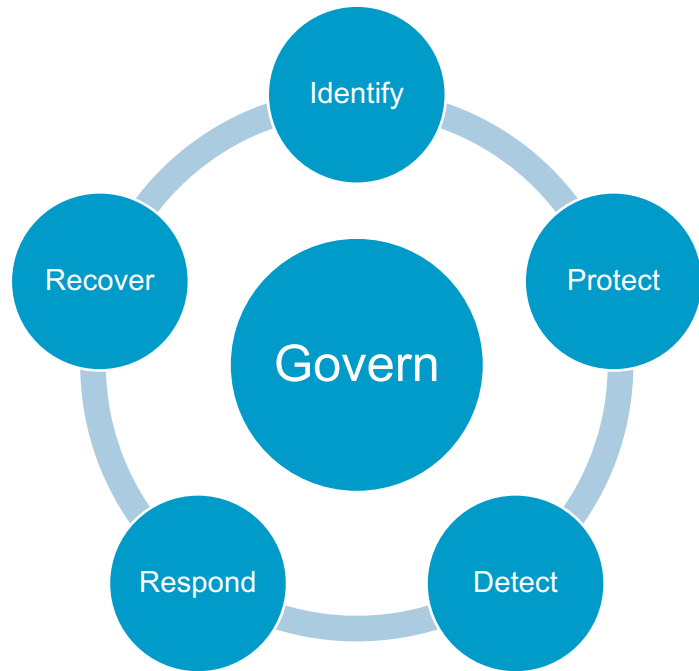
Overview

Vue d'ensemble



NIST CSF 2.0

NIST Cadre de cybersécurité 2.0



CASL LCAP

Canada's anti-spam legislation

La Loi canadienne anti-pourriel

The image displays two overlapping screenshots of the Government of Canada website. The top screenshot shows the English version of the page titled "Canada's anti-spam legislation". The bottom screenshot shows the French version titled "La Loi canadienne anti-pourriel". Both pages feature a header with the Government of Canada logo and a search bar. The main content area includes a banner with icons of a laptop and a smartphone, followed by introductory text and several sections with sub-headers and bullet points. The English page includes sections for "Report spam", "Protect your business and comply", "Canada's anti-spam legislation resources", "What is spam?", and "Resources pour la Loi canadienne anti-pourriel". The French page includes sections for "Signaler un pourriel", "Nouvelles sur les pourriels", "Protégez-vous des pourriels", "Comprendre la Loi canadienne anti-pourriel", and "Répondez à notre questionnaire sur les pourriels".

PIPEDA LPRPDE

The Personal Information Protection and Electronic Documents Act

La Loi sur la protection des renseignements personnels et les documents électroniques

The screenshot displays the official website of the Office of the Privacy Commissioner of Canada. The page is presented in French, with the title "La Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)". The layout includes a top navigation bar with links for individuals, businesses, and federal institutions. The main content area is divided into several sections: "Features" with a "Privacy Guide for Businesses" link, "Legislative reform" with a link to "Submissions to parliament, recommendations", and "En vedette" (Featured) with a link to "10 conseils de protection de la vie privée pour les entreprises". The page also features a search bar and a language selector (English/Français).

CPCSC PCCC

Canadian program for cyber security certification

Programme canadien de certification en cybersécurité

The screenshot displays the Government of Canada website in English. The main heading is "Cyber security certification for defence suppliers in Canada". Below the heading, there is a sub-heading "Explore upcoming cyber security requirements for defence suppliers in Canada" and a search bar. The page is divided into several sections:

- On this page:** A list of links including "About upcoming changes", "Overview of program", "Certification levels", "Benefits for Canada", "Benefits for suppliers", "Timing of upcoming requirements", "Contact us", "Resources for suppliers", and "Related links".
- About upcoming changes:** A section titled "About upcoming changes" with a sub-heading "Beginning at the end of 2024, suppliers will become certified under the Canadian Cyber Security Program (CCSP) to strengthen cyber security." It includes a link to "Canadian Program for Cyber Security".
- Canadian Program for Cyber Security:** A section titled "Canadian Program for Cyber Security" with a sub-heading "Public Services and Procurement Canada is seeking input from suppliers through participation in the Request for Information (RFI) on the development and implementation of the program." It includes a link to "The RFI is scheduled to close on June 28, 2024. Information - Tender Notice".
- Overview of program:** A section titled "Overview of program" with a sub-heading "Once in place, the CCSP will aim to:" and a list of bullet points including "protect federal contractual information".
- Certification des fournisseurs du secteur de la défense au Canada concernant la cybersécurité:** A section titled "Certification des fournisseurs du secteur de la défense au Canada concernant la cybersécurité" with a sub-heading "Renseignez-vous sur les nouvelles exigences en matière de cybersécurité qui s'appliqueront aux fournisseurs qui soumissionnent les contrats de défense du gouvernement du Canada ou y travaillent. Ces exigences visent à protéger les réseaux, les systèmes et les applications contre les cyberactivités malveillantes." It includes a link to "Demande de Renseignements du Programme Canadien de Certification en Cyber Sécurité Maintenant Disponible sur CanadaAchats".
- À propos des changements à venir:** A section titled "À propos des changements à venir" with a sub-heading "À compter de la fin de 2024, les fournisseurs qui souhaitent soumissionner certains contrats de défense du gouvernement du Canada ou y travailler devront détenir une certification du programme canadien de certification en cybersécurité (PCCC). Le PCCC viendra compléter les efforts que nous déployons pour renforcer la cybersécurité. Il le fera en resserrant la sécurité du processus de passation des contrats du gouvernement fédéral." It includes a link to "Demande de Renseignements du Programme Canadien de Certification en Cyber Sécurité Maintenant Disponible sur CanadaAchats".

ISO 27001 : 2022

Information Security Management System (ISMS)

- Policies
- Procedures
- Standards
- Guidelines

Système de gestion de la sécurité de l'information (SGSI)

- Politiques
- Procédures
- Normes
- Lignes directrices

BC PIPA

The Personal Information Protection Act

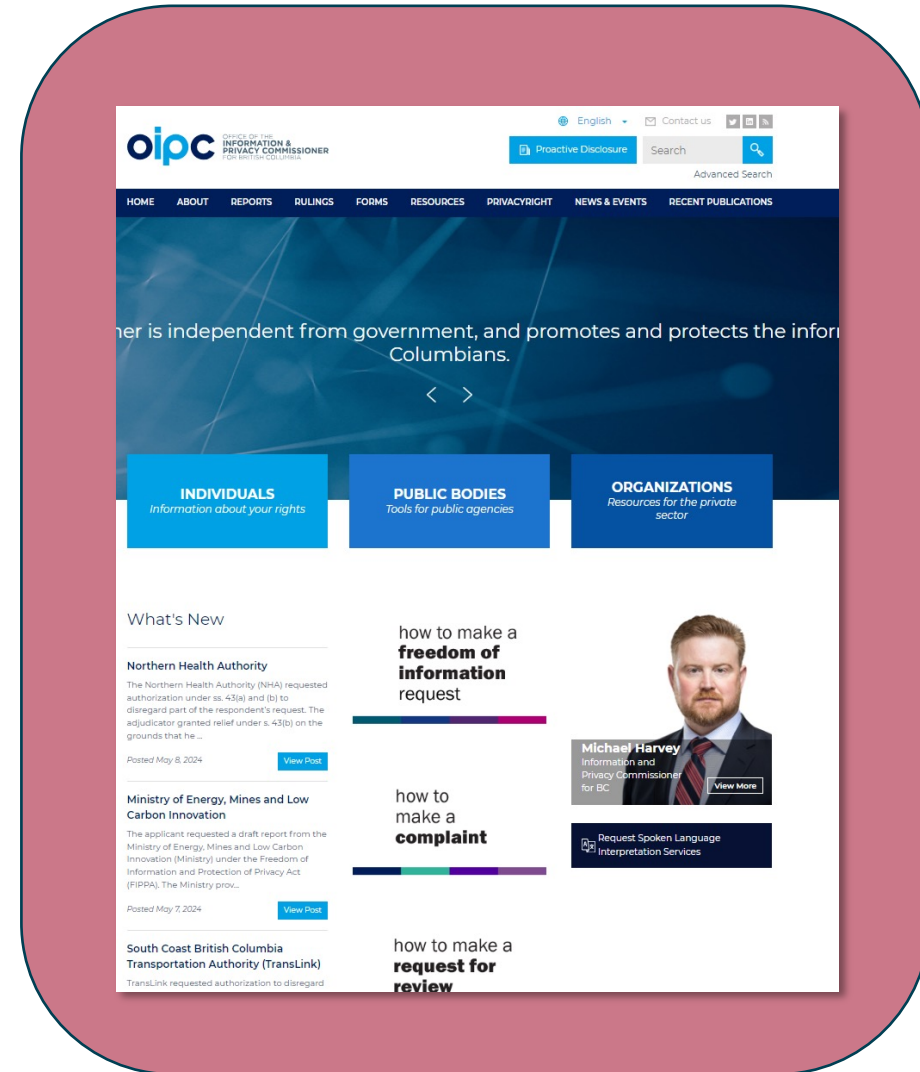
La loi sur la protection des renseignements personnels

The screenshot displays the website of the Office of the Information & Privacy Commissioner for British Columbia (OIPC). The page is titled "A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations" and is dated October 2015 (5th publication). The page features a navigation menu with links to HOME, ABOUT, REPORTS, RULINGS, FORMS, RESOURCES, PRIVACYRIGHT, NEWS & EVENTS, and RECENT PUBLICATIONS. The main content area includes a section for "ORGANIZATIONS" with the subtitle "Resources for the private sector" and a brief description of the Personal Information Protection Act. Below this, there are three featured articles: "PrivacyRight: Fundamentals for business", "Guide to...", and "Security". The page also includes a search bar, a language selector (English), and a contact us link. The footer contains the OIPC logo and the tagline "Protecting privacy. Promoting transparency."

BC FIPPA

Freedom of Information and Protection of Privacy Act

La loi sur la protection des renseignements personnels



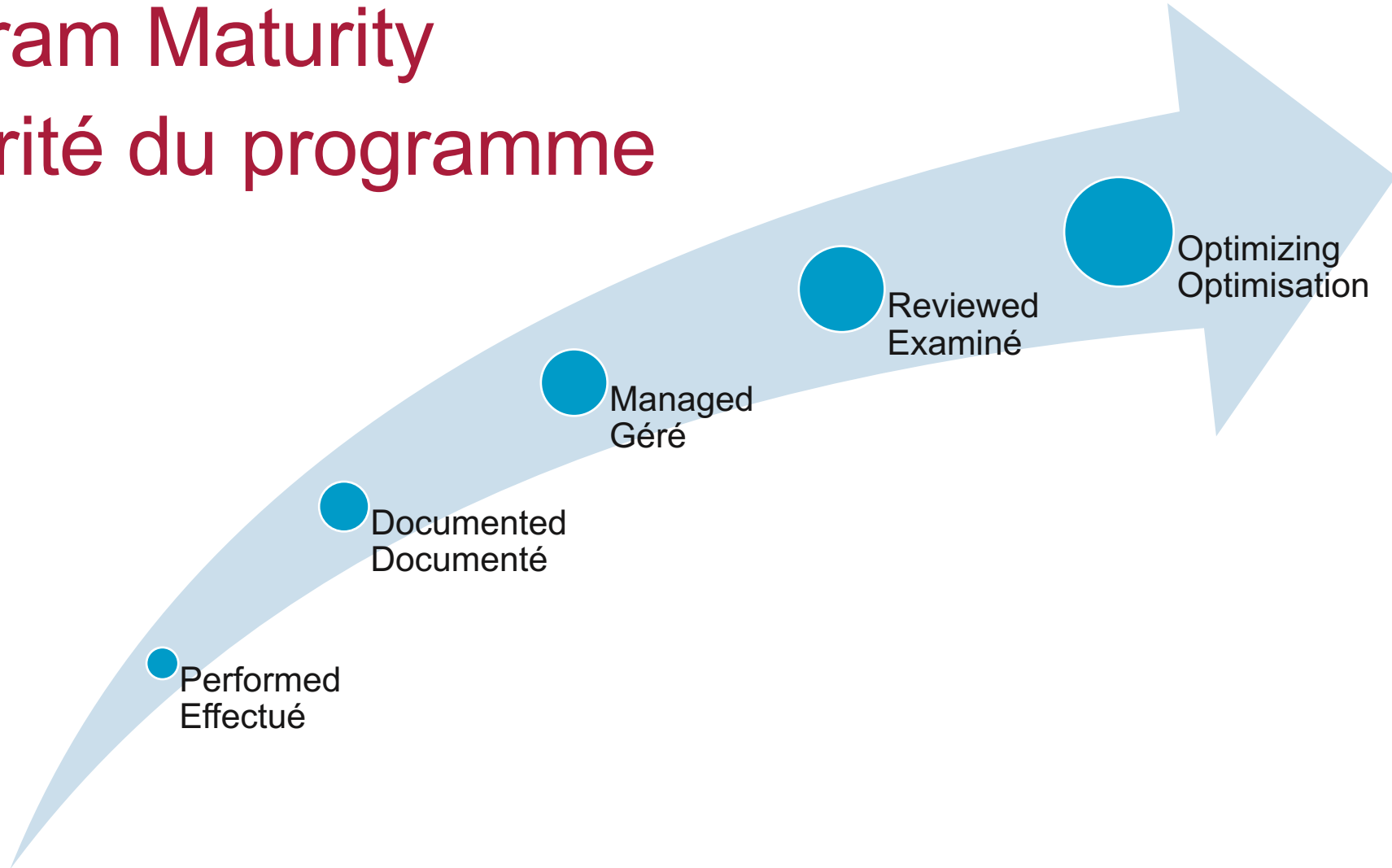


Data Security Policies

Politiques de sécurité des données

Program Maturity

Maturité du programme



ISO 27001 : 2022

Information Security Management System (ISMS)

- Policies
- Procedures
- Standards
- Guidelines

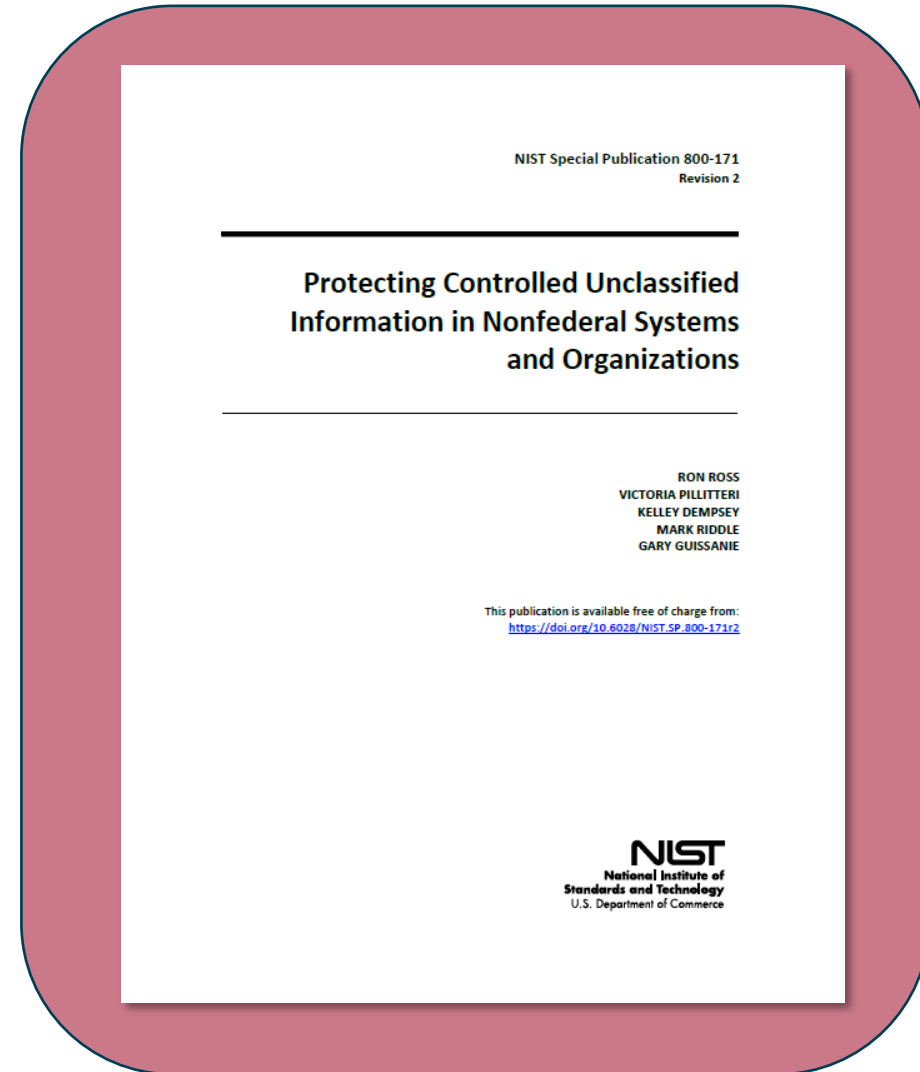
Système de gestion de la sécurité de l'information (SGSI)

- Politiques
- Procédures
- Normes
- Lignes directrices

NIST SP 800-171 r2

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Protection des informations non
classifiées contrôlées dans les
systèmes et organisations non
fédéraux





Incident Management Gestion des incidents

Before Avant

Incident Response Plan

- Assess
- Develop
- Educate
- Communicate
- Exercise
- Optimize

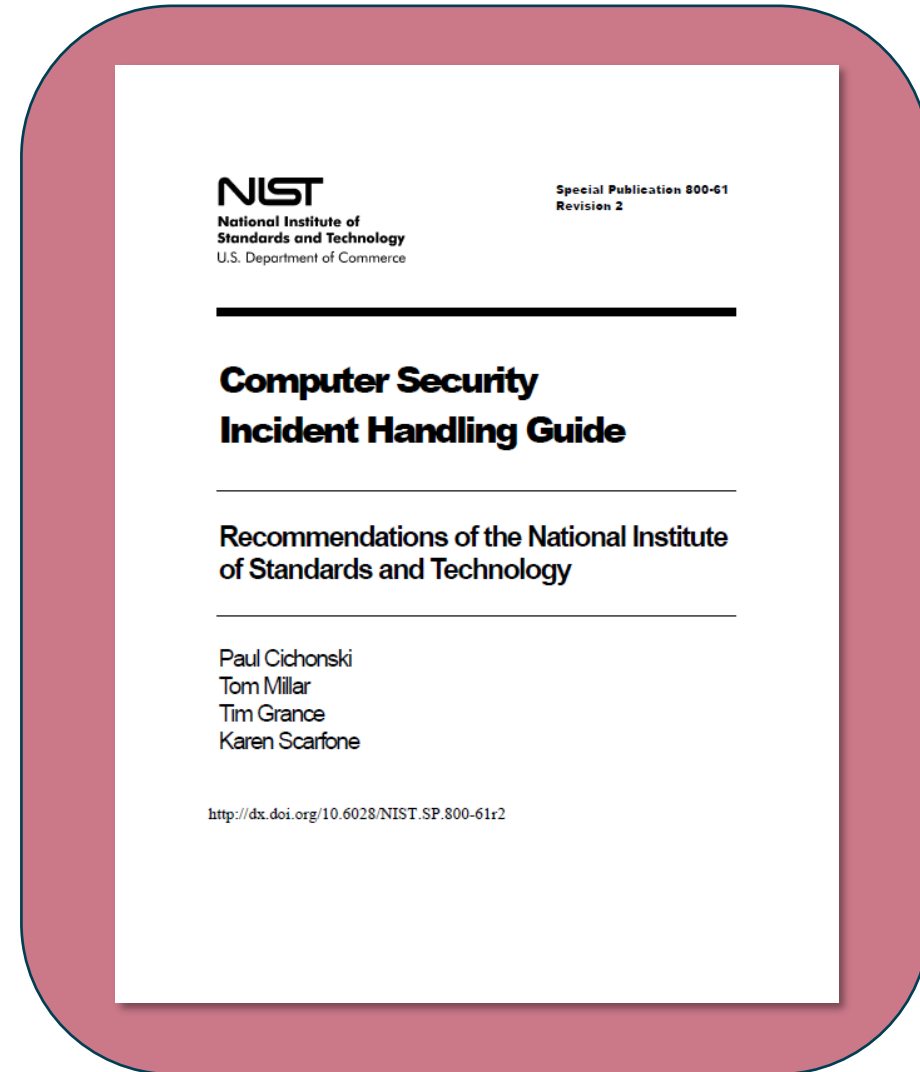
Plan d'intervention en cas d'incident

- Évaluer
- Développer
- Éduquer
- Communiquer
- Exercice
- Optimiser

NIST SP 800-61 r2

Cyber Security Incident Handling Guide

Guide de traitement des incidents de cybersécurité



NIST SP 800-61 r2

Cyber Security Incident Handling Guide

Guide de traitement des incidents de cybersécurité

Handling an Incident.....

- 3.1 Preparation.....
 - 3.1.1 Preparing to Handle Incidents
 - 3.1.2 Preventing Incidents.....
- 3.2 Detection and Analysis.....
 - 3.2.1 Attack Vectors.....
 - 3.2.2 Signs of an Incident.....
 - 3.2.3 Sources of Precursors and Indicators.....
 - 3.2.4 Incident Analysis.....
 - 3.2.5 Incident Documentation.....
 - 3.2.6 Incident Prioritization.....
 - 3.2.7 Incident Notification.....
- 3.3 Containment, Eradication, and Recovery.....
 - 3.3.1 Chc
 - 3.3.2 Evic
 - 3.3.3 Ider
 - 3.3.4 Era
- 3.4 Post-Inciden.....
 - 3.4.1 Les
 - 3.4.2 Usii
 - 3.4.3 Evic
- 3.5 Incident H
- 3.6 Recommer

Table 3-5. Incident Handling Checklist

Action		Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
4.	Acquire, preserve, secure, and document evidence	
5.	Contain the incident	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, and other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

During Au cours de

Keys to Success

1. Make a formal declaration
2. Engage stakeholders and partners
3. Follow the plan
4. Document everything

Les clés du succès

1. Faites une déclaration formelle
2. Engagez les partenaires
3. Suivez le plan
4. Documentez tout

After Après

Recovery

- People
- Process
- Technology
- Data
- Reputation

Récupération

- Les gens
- Processus
- La technologie
- Données
- Réputation

Cyber Risk Insurance

Assurance contre les cyberrisques

Challenges

- New, more rigorous requirements
- Limited list of acceptable security partners
- New scrutiny and limitations on payouts

Problèmes

- De nouvelles exigences plus rigoureuses
- Liste limitée de partenaires de sécurité acceptables
- Nouvel examen et limites sur les paiements

Partners for Government Agencies

Partenaires pour les organismes gouvernementaux

CANADIAN CENTRE FOR
CYBER SECURITY

CENTRE CANADIEN POUR
LA
CYBERSÉCURITÉ





THANK YOU FROM CIRA

Jamie Hari

Director of Product, Cyber/DNS

 @jamie_hari

 [linkedin.com/in/jamiehari](https://www.linkedin.com/in/jamiehari)

 www.cira.ca

 info@cira.ca

Thank you.

JAMIE HARI | Director / Directeur, CyberDNS
Jamie.hari@cira.ca



FACEBOOK /cira.ca
INSTAGRAM /ciradotca
MASTODON /@cira
X /ciranews

TIKTOK /@cira.ca
YOUTUBE /ciranews
LINKEDIN /company/canadian-internet-registration-authority

Settlement Spotlight Newsletter

Bulletin d'information Pleins feux sur
l'établissement

Follow AMSSA on Social Media

@amssabc on X and Facebook

AMSSA on LinkedIn



Suivez-nous sur les médias sociaux

@amssabc sur X et Facebook

AMSSA sur LinkedIn

