Privacy and Security Risk Management Framework

Canadian Institute for Health Information
Institut canadien d'information sur la santé

Production of this document is made possible by financial contributions from Health Canada and provincial and territorial governments. The views expressed herein do not necessarily represent the views of Health Canada or any provincial or territorial government.

Unless otherwise indicated, this product uses data provided by Canada's provinces and territories.

Canadian Institute for Health Information
495 Richmond Road, Suite 600
Ottawa, Ontario K2A 4H6
Phone: 613-241-7860
Fax: 613-241-8120
cihi.ca
copyright@cihi.ca

How to cite this document:
Canadian Institute for Health Information. *Privacy and Security Risk Management Framework*. Ottawa, ON: CIHI; 2020.

Cette publication est aussi disponible en français sous le titre *Cadre de gestion des risques liés au respect de la vie privée et à la sécurité*.

Table of contents

1 Introduction

1.1 Overview

Privacy and security risk management (PSRM) is a formal, repeatable process for identifying, assessing, treating and monitoring risks in order to minimize the probability of such risks materializing and/or their impact should they occur.

This PSRM Framework provides an overview of PSRM at the Canadian Institute for Health Information (CIHI), including its alignment with CIHI's Corporate Risk Management Framework, drivers for PSRM, the governance model, CIHI's risk tolerance and the PSRM methodology.

2 Alignment with Corporate Risk Management Framework

This PSRM Framework has been designed to integrate and align with CIHI's Corporate Risk Management Framework, shown below:

PSRM informs and aligns with corporate risk management activities through

- Adopting a similar methodology, terminology and governance structure; and
- Identifying privacy and security risks for potential inclusion on the Corporate Risk Register.

3 Why PSRM?

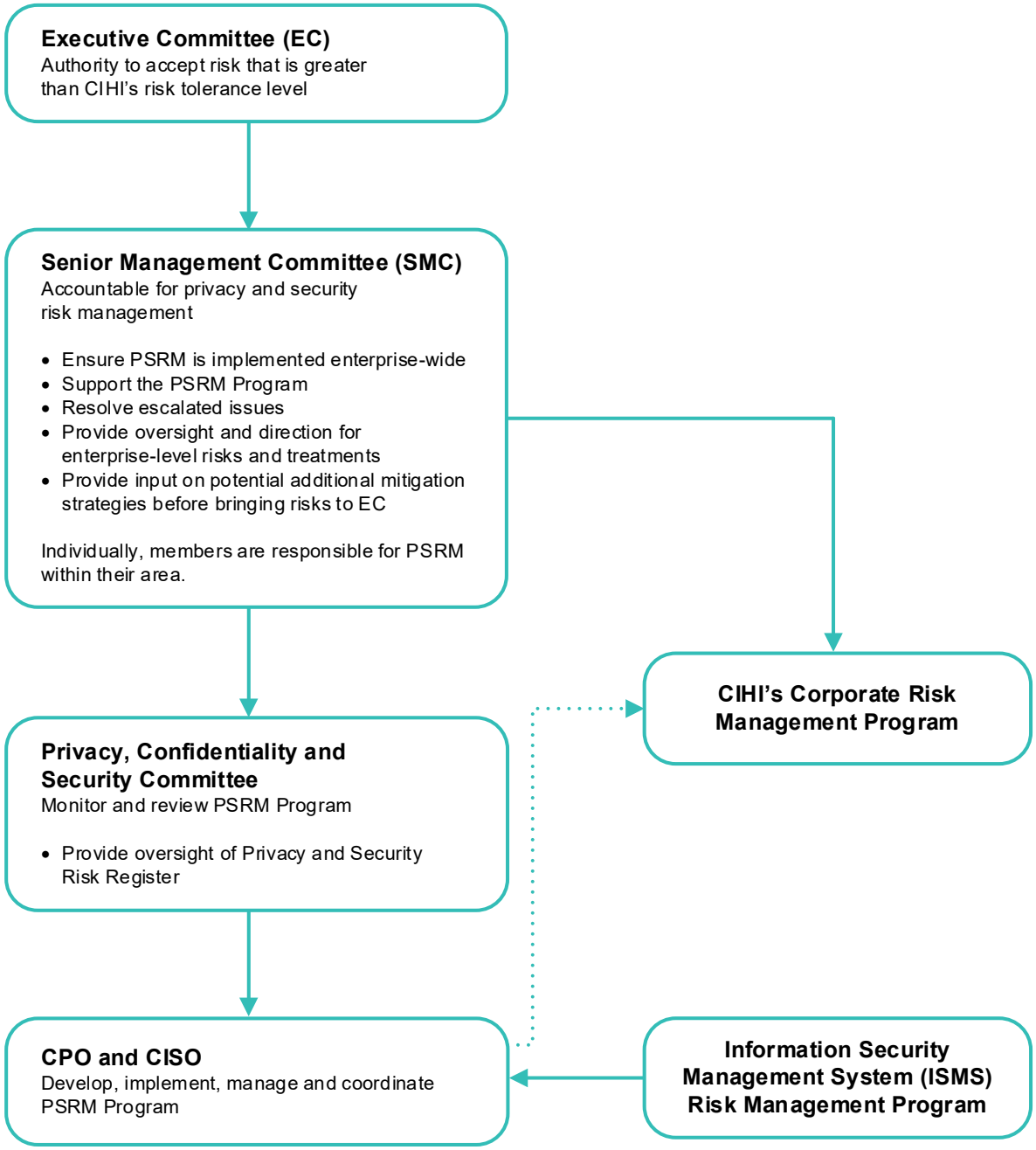
Effective management of privacy and security risks is essential for CIHI to achieve its strategic goals and is a core requirement for CIHI's continued designated status under the *Personal Health Information Protection Act* (PHIPA) of Ontario.

Adopting an effective and robust PSRM program contributes to stakeholder and public trust by demonstrating CIHI's commitment to protecting the personal health information that it maintains.

By implementing a continuous, proactive and systematic process to understand, manage and communicate privacy and security risks, CIHI can make sound strategic and tactical decisions based on real risk, cost and benefit.

4 Risk management governance

CIHI's chief privacy officer (CPO) and chief information security officer (CISO) have primary responsibility for CIHI's PSRM Program. CIHI has defined management responsibilities and a governance framework for effective PSRM, as shown in the figure below.



5 CIHI's risk tolerance

It is not always efficient or possible to eliminate risk due to the time, cost or effort that would be required, or because of other constraints. On the other hand, risks that are clearly inconsistent with CIHI's vision, mandate and strategic goals may not be acceptable. On this basis, CIHI has developed a privacy and security risk tolerance statement that sets out the amount of residual risk it is willing to bear as part of normal management practice.

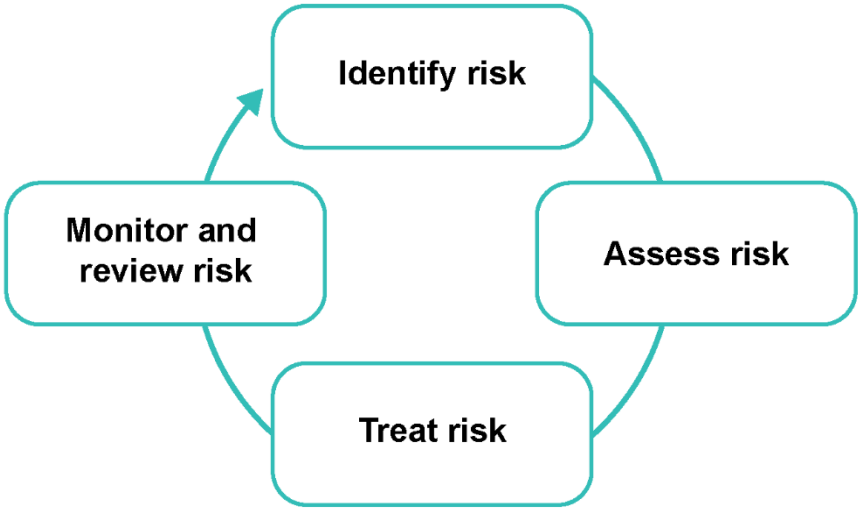
CIHI is willing to accept risk that

- May result in minor delays in achieving CIHI's objectives;
- Does not lead to financial losses;
- May result in some potential for minor complaints, non-compliance issues or negative media coverage;
- May lead to some impact on public perception;
- May cause low stakeholder concern; and
- May lead to a potential minimal impact on service delivery.

The consequences of the risk event could be absorbed by normal activity or with minimal effort.

CIHI's privacy and security risk tolerance: **LOW**

6 PSRM methodology



CIHI's PSRM methodology is made up of the following 4 steps:

1. **Identify risk:** Risks are identified through a variety of sources and are entered into the Privacy and Security Risk Register.
2. **Assess risk:** Risk likelihood and impact are assessed in order to determine whether risk treatment is required. Risks that are within CIHI's identified risk tolerance require no treatment.
3. **Treat risk:** Options for risk treatment are mitigating the risk, transferring the risk, avoiding the risk or accepting the risk.
4. **Monitor and review risk:** Risks and risk treatments must be continually monitored to ensure that CIHI's assets are adequately protected.

Appendix: Text alternative for figures

Text alternative for CIHI's Corporate Risk Management Framework

The first process is Establish framework (which involves the policy and governance frameworks, as well as the process, methods and tools). The second process is Assess the risks (which involves identification of strategic goals and risks, as well as risk assessment). The third process is Risk response and treatment (which involves key risk indicators, strategy and action plans, and risk champions). The fourth process is Monitor and communicate (which involves reviewing the framework, Executive and Board oversight and risk management reporting).

Text alternative for governance framework

CIHI's Executive Committee (EC) has the authority to accept risk that is greater than CIHI's risk tolerance level.

The Senior Management Committee (SMC) is accountable for privacy and security risk management. It

- Ensures PSRM is implemented enterprise-wide;
- Supports the PSRM Program;
- Resolves escalated issues;
- Provides oversight and direction for enterprise-level risks and treatments; and
- Provides input on potential additional mitigation strategies before bringing risks to EC.

Individually, members are responsible for PSRM within their area.

The Privacy, Confidentiality and Security Committee monitors and reviews the PSRM Program and provides oversight of the Privacy and Security Risk Register.

The CPO and CISO develop, implement, manage and coordinate the PSRM Program.

SMC and the CPO and CISO both provide input into CIHI's Corporate Risk Management Program.

CIHI's Information Security Management System (ISMS) Risk Management Program informs the PSRM.

help@cihi.ca

CIHI Ottawa
495 Richmond Road
Suite 600
Ottawa, Ont.
K2A 4H6
613-241-7860

CIHI Toronto
4110 Yonge Street
Suite 300
Toronto, Ont.
M2P 2B7
416-481-2002

CIHI Victoria
880 Douglas Street
Suite 600
Victoria, B.C.
V8W 2B7
250-220-4100

CIHI Montréal
1010 Sherbrooke Street West
Suite 602
Montréal, Que.
H3A 2R7
514-842-2226

cihi.ca

22660-0720