Infrastructure Canada

# Infrastructure Canada

## Internal Audit of the Cyber Security Framework

**June 2024**

Canada

This publication is available upon request in accessible formats.
Contact:
Communications Branch
Infrastructure Canada
180 Kent Street, Suite 1100
Ottawa, Ontario K1P 0B6

National information line on infrastructure: 613-948-1148
Toll free number: 1-877-250-7154
TTY: 1-800-465-7735
Email: infc.info.infc@infc.gc.ca

This publication is available at
https://www.infrastructure.gc.ca/pd-dp/ia-vi/index-eng.html



Cat. No. T94-64/2024E-PDF

ISBN 978-0-660-71884-2

Aussi disponible en français sous le titre : *Audit interne du cadre de cybersécurité*

# Table of Contents

# EXECUTIVE SUMMARY

## BACKGROUND

Cyber security is ever evolving, and the threat of bad actors working to obtain information, compromise network devices, and undermine secure processes is constant. The risk of a cyber-attack looms large for all departments and agencies across the Government of Canada, and Infrastructure Canada (INFC) is no exception. INFC has an opportunity to respond to growing threats and foster a strong, resilient, and responsive cyber security landscape through an established cyber security framework.

## OBJECTIVE

This internal audit is an assurance engagement which intends to determine whether INFC has effective management control processes in place in order to identify, respond, mitigate, and recover from cyber security vulnerabilities, incidents, and risks, as well as an assessment on whether the measures taken are in compliance with applicable Treasury Board (TB) policy requirements.

## OVERALL OBSERVATIONS

- The cyber security framework at INFC is part of an integrated security program, and as such, is at a development stage which requires many essential governance artifacts. The cyber security framework should be further developed, formalized and better structured to address monitoring, reporting and approvals, inter-departmental dependencies and prioritization processes, respectively.
- While controls surrounding INFC's cyber security framework are in place to support cyber security operations, there is an opportunity to further improve efficiency to ensure the proper functioning of an effective framework.
- In addition, it would be beneficial to examine INFC's awareness surrounding its level of confidence to respond to potential cyber security risks and in doing so, formulate a change management plan to improve the organization's awareness posture.

## OVERALL CONCLUSION

This internal audit concluded, with reasonable assurance that, INFC has effective management control processes in place to identify, respond, mitigate and recover from cyber security vulnerabilities, incidents, and risks and is generally compliant with applicable TB policies and directives. Some opportunities for improvement exist to further enhance INFC's cyber security framework, as part of the Department's overall integrated security program, especially related to improving the efficiency of governance, operational processes and inter-departmental risk mitigation strategies.

As a result, the following recommendations directed at INFC's Information Management and Information Technology Directorate (IMITD) are, notably:

1. The governance and oversight processes surrounding the development and finalization of a cyber security framework (including the Security Assessment and Authorization process), should be updated with a view to further improve efficiency and compliance with applicable TB policies and directives, as well as industry standards. Notably:

a. To review, recalibrate and formalize the structure and membership of oversight committees to ensure appropriate approvals and assessments of projects and initiatives; and,

b. That monitoring processes and reporting capabilities continue to be revised to improve security posture awareness that supports an informed decision-making process.

2. Operational readiness to respond to potential cyber security incidents should be augmented and optimized (including mandatory training requirements), to ensure continued departmental awareness and protection of INFC's IT environment, respectively, including the safeguarding of data and assets.

3. Dependencies on service providing departments should be reassessed to ensure a formal agreement is in place that aligns with the Department's overall business continuity plan (BCP) objectives, especially as it relates to information management and information technology (IM/IT) needs and expectations, where appropriate.

# BACKGROUND

Cyber security is ever evolving, and the threat of bad actors working to obtain information, compromise network devices, and undermine secure processes is constant. The risk of a cyber-attack looms large for all departments and agencies across the Government of Canada (GoC), and Infrastructure Canada (INFC) is no exception.

Cyber-attacks at INFC could result in significant data breaches and operational stand-stills, including but not limited to:

- Preventing internal staff and external stakeholders from accessing information which may cause operational disruptions (e.g., including but not limited to business and financial management);
- Limiting staff from continuing with their operations (e.g., ranging from administration to performance monitoring/reporting issues); and,
- Failure to meet stakeholder program needs and services (e.g., impacting stakeholder/ partnership relations with Provinces, Territories, and Municipalities).

INFC has an opportunity to respond to growing threats and foster a strong, resilient, and responsive cyber security landscape through a dedicated cyber security framework, deriving from the assessment of its framework, which took place in October 2022.

The Information Management (IM) and Information Technology (IT) Directorate (IMITD) at INFC is responsible for IT and cyber security services. IT Security, specifically, oversees the security of electronic information and assets that are stored, processed or transmitted on electronic systems. This unit plays an integral part of a continuous program and service delivery that needs to be viewed as an "enabler" to support the business of INFC, while collaborating and coordinating with the Canadian Centre for Cyber Security (CCCS) and Shared Services Canada (SSC), given the reliance on SSC to support some of INFC's IT infrastructure and ensure its security.

# AUDIT OBJECTIVE AND SCOPE

## OBJECTIVE

This internal audit is an assurance engagement which intends to determine whether INFC has effective management control processes in place in order to identify, respond, mitigate and recover from cyber security vulnerabilities, incidents, and risks, as well as an assessment on whether the measures taken are in compliance with applicable Treasury Board (TB) policy requirements.

## SCOPE

The internal audit examined the following three main categories: governance of cyber security; cyber security operational readiness; and risks, dependencies, and inter-dependencies around cyber security.

## STATEMENT OF CONFORMANCE

This internal audit conforms with the Institute of Internal Auditors' International Standards for the Professional Practice of Internal Auditing, as supported by the last results of the Quality Assurance and Improvement Program.

A detailed methodology and approach can be found in Annex B.

## AUDIT CRITERIA

1. Governance - Governance structures are in place that support the strategic and administrative cyber security framework processes.
2. Operational Readiness - Controls are in place and monitored to support cyber security operations.
3. Risks, Dependencies and Inter-Dependencies - The IMIT Directorate (IMITD, within Corporate Services Branch (CSB)) led by the Chief Information Officer (CIO) understands its cyber security risks to operations and business processes.

# CONCLUSION AND OBSERVATIONS

## CONCLUSION

This internal audit concluded, with reasonable assurance, that INFC has effective management control processes in place to identify, respond, mitigate and recover from cyber security vulnerabilities, incidents, and risks and is generally compliant with applicable TB policies and directives. Some opportunities for improvement exist to further enhance INFC's cyber security framework, as part of the Department's overall integrated security program, especially related to improving the efficiency of governance, some operational processes and inter-departmental risk mitigation strategies.

## OBSERVATIONS SUMMARY

The internal audit examined the following three main areas (per Annex C) governance of cyber security; cyber security operational readiness; and risks, dependencies, and inter-dependencies around cyber security, to determine whether processes in place were working as intended.

# OBSERVATIONS

## 1. GOVERNANCE

Cybersecurity governance requires a balanced approach to respond in an agile structure to new and emerging threats and, at the same time, demonstrate resiliency through a substantive and structured framework. This internal audit sought to determine whether IMITD had struck a successful balance between agility and structure and opine on potential areas of improvement. To that end, this internal audit examined the following three sub-criteria:

1.1 A cyber security framework exists, is well-socialized, and available for access throughout the organization.

1.2 Governance structures (committees, working groups, etc.) and processes are established and implemented to ensure effective oversight.

1.3 Roles and responsibilities are well defined, documented, communicated, understood, and operating as intended.

**Finding:** The internal audit found that INFC's Information Management Information Technology Directorate (IMITD) has benefited greatly from a governance approach that has prioritized agile adaptation to its decision-making process, security assessments and reporting. As such, IMITD's governance system has enabled the cybersecurity team to respond nimbly to emerging threats, and to manage INFC's cyber assets effectively. However, it was noted that, in some instances, there was a lack of formal documentation and oversight.

**Impact (i.e. what could happen if the finding is not addressed):** The lack of consistency and formal governance structures in key areas may create vulnerabilities by allowing processes to be applied inconsistently. Moreover, a lack of clear governance structures may create situations where concerns around core processes are not always elevated to respective stakeholders and decision makers.

**Recommendation #1:** It is recommended that the ADM, Corporate Services, in consultation with the CIO, update the governance and oversight processes surrounding the development and finalization of a cyber security framework (including the Security Assessment and Authorization process), with a view to further improve efficiency and compliance with applicable TB policies and directives, as well as industry standards. Notably:

a) To review, recalibrate and formalize the structure and membership of oversight committees to ensure appropriate approvals and assessments of projects and initiatives; and,

b) That monitoring processes and reporting capabilities continue to be revised to improve security posture awareness that supports an informed decision-making process.

## 2. OPERATIONAL READINESS

This area examined operational readiness, to determine the extent to which INFC could defend against cyber threats, whereby, a robust plan that encompasses the following should be in place- technology, resources and a security-aware culture. As such, the internal audit examined the following three sub-criteria:

2.1 Incident management standard operating procedures/protocols exists and are operating effectively.

2.2 Adequate resources and supporting technologies are in place to effectively respond to cyber security incidents.

2.3 Security posture monitoring and reporting are conducted in a consistent, on-going manner, which informs and supports decision-making processes.

**Finding:** The internal audit found the Information Management Information Technology Directorate (IMITD) responds well to cyber security threats and is actively working to minimize known risks. Education programs like their phishing campaigns are working to elevate security awareness, while partnerships with SSC have provided the Department with high performance tools to manage INFC's cyber space. However, as the cyber security landscape continues to evolve and intensify, there is a continued need for INFC to augment and optimize its defense capabilities.

**Impact (i.e. what could happen if the finding(s) is not addressed):** INFC's IT assets, if compromised in a cyber-attack, may result in potential financial, human and reputational damage.

**Recommendation #2:** It is recommended that the ADM, Corporate Services, in consultation with the CIO, augment and optimize its operational readiness (including mandatory training requirements) to respond to potential cyber security incidents, to ensure continued departmental awareness and protection of INFC's IT environment, respectively, including the safeguarding of data and assets.

## 3. RISKS, DEPENDENCIES, AND INTER-DEPENDENCIES

Part of an organization's security defense armour is the holistic view and understanding of internal risks as it pertains to dependencies and inter-dependencies with partner agencies and other service-providing departments within the Government of Canada landscape. As such, the internal audit examined the following two sub-criteria surrounding INFC's cyber security environment (IM/IT ecosystem):

3.1 IMITD understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

3.2 IMITD's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Finding: The internal audit found that the Information Management Information Technology Directorate (IMITD) has a good understanding of the cyber security threat landscape and follows an integrated security approach to address risks and priorities facing its operational decisions. However, in some cases, INFC is consuming services offered by service providing departments without established service level agreements; as well, a misalignment exists between established SLAs and INFC's business continuity plan.

**Impact (i.e. what could happen if the finding(s) is not addressed):** Misalignment between established service level agreements and business continuity plan objectives may cause prolonged disruptions and/or outages in an emergency scenario, further impacting the administration/management of INFC programs.

**Recommendation #3:** It is recommended that the ADM, Corporate Services, in consultation with the CIO, reassess dependencies on service providing departments to ensure a formal agreement is in place, that aligns with the Department's overall BCP objectives, especially as it relates to IM/IT needs and expectations, where appropriate.

# ANNEXES

## ANNEX A – MANAGEMENT ACTION PLAN

| Recommendation | Management Response and Action Plan | Key Deliverables | OPI and due date |
|---|---|---|---|
| 1. The governance and oversight processes surrounding the development and finalization of a cyber security framework (including Security Assessment & Authorization (SA&A) process) should be updated with a view to further improve efficiency and compliance with applicable Treasury Board (TB) policies and directives, as well as industry standards. Notably:<br><br>a) To review, recalibrate and formalize the structure and membership of oversight committees to ensure appropriate approvals and assessments of projects and initiatives; and,<br><br>b) That monitoring processes and reporting capabilities continue to be revised to improve security posture awareness that supports an informed decision-making process. | Agreed. A holistic review of the cyber security governance structure will be conducted to formalize the governance structure, enhance decision making processes and improve security posture reporting. | a) Review governing committees' structure with a goal to establish formal TOR(s) for such committees or disband/replace them accordingly.<br><br>b) Review the SA&A process and enact controls to ensure that the process adheres to INFC's guidelines as well as the principles outlined in the Canadian Centre for Cyber Security's Information Technology Security Guidance.<br><br>c) Review reporting capabilities and establish reporting mechanisms to inform senior management of the overall security posture at INFC. | a) IMITD: 07-31-2024<br><br>b) IMITD: 09-30-2024<br><br>c) IMITD: 12-31-2024 |

| | | | |
|---|---|---|---|
| 2. Operational readiness to respond to potential cyber security incidents should be augmented and optimized (including mandatory training requirements), to ensure continued departmental awareness and protection of INFC's IT environment, respectively, including the safeguarding of data and assets. | Agreed. The cyber security team will assess current and in-flight (projects in motion) defence capabilities to ensure INFCs digital assets are well protected. Moreover, the cyber team will review its incident response framework and processes. | a) Ensure that IT-related training, especially around phishing prevention, is mandatory as part of all INFC's employees' personal learning plans.<br>b) Update the INFC Cyber Security Event Management Plan and Incident Response Plan.<br>c) Develop a framework governing the protection and safeguarding of INFC's data, which includes: DLP policy and associated standard operating procedure document to ensure consistent approach of the implementation of DLP capabilities within the INFC IT environment. | a) IMITD: 07-31-2024<br>b) IMITD: 08-31-2024<br>c) IMITD: 12-31-2024 |
| 3. Dependencies on service providing departments should be reassessed to ensure a formal agreement is in place that aligns with the Department's overall business continuity plan (BCP) objectives, especially as it relates to information management and information technology (IM/IT) needs and expectations, where appropriate. | Agreed. The INFC cyber security and IT Operations teams will assess INFC's reliance on third-party vendors whether external or internal service providing departments, to ensure alignment with departmental IT expectations. | a) Where possible, establish service level agreements (SLA) with all departments that provide a platform or an IT service to INFC; and,<br>b) Align INFC's BCP documents with established SLAs to reflect operational realities that are in line with INFC's risk appetite. | a) IMITD: 03-31-2025<br>b) IMITD: 03-31-2025 |

# ANNEX B – INTERNAL AUDIT METHODOLOGY

In accordance with INFC's approved 2023-2028 IAEP, the Audit and Evaluation Branch undertook the Audit of INFC's Cyber Security Framework.

## RISK ASSESSMENT

A risk-based approach was used to establish the objectives, scope, and approach for this internal audit. The same was used to provide timely assurance of the effectiveness of selected core controls. The audit performed a targeted review using a limited sample of items relevant to the INFC's IT environment, especially, as it relates to cyber security; therefore, the audit results cannot be extrapolated. It is not a fully comprehensive assessment of all internal controls that exist.

Considering these risks, detailed audit criteria and sub-criteria (found in Annex C) were developed to guide the audit field work and form the basis for the overall internal audit's conclusion.

## DOCUMENT REVIEW, INTERVIEWS, AND WALKTHROUGH

The internal audit included various tests, as considered necessary, to provide reasonable assurance on the overall internal audit conclusion.

These tests included, but were not limited to, interviews, walkthroughs, a review and analysis of applicable GoC and TB policies, directives, guidelines, related industry standards, as well as other supporting documentation and audit procedures. All project files were reviewed as part of the testing procedures.

The field work was substantially completed on December 31, 2023.

This internal audit findings were communicated to the office of primary interest/auditee to validate facts and to confirm the clarity, accuracy, and completeness of the information reported.

## SCOPE LIMITATIONS

Based on preliminary planning activities, the overall period covered by this internal audit included activities performed as part of INFC's cyber security framework assessment between January 1, 2022 and December 31, 2023.

The audit, in particular, examined the following three main areas (criteria):

1. Governance of cyber security;
2. Cyber security operational readiness; and
3. Risks, dependencies, and inter- dependencies around cyber security.

The audit did not examine artificial intelligence readiness, nor evaluate at a granular technical level, any specific cyber security tools currently deployed in the environment; however, examined the existence of appropriate solutions utilized, as part of the cyber security operational readiness.

# ANNEX C – ENGAGEMENT CRITERIA AND SUB-CRITERIA

In support of the audit objective and following the risk assessment of the entity/program, the following criteria and sub-criteria were developed. These sub-criteria guided the audit fieldwork and form the basis for the overall audit conclusion.

1. Governance - Governance structures are in place that support the strategic and administrative cyber security framework processes.

    1.1 A cyber security framework exists, is well-socialized, and available for access throughout the organization.

    1.2 Governance structures (committees, working groups, etc.) and processes are established and implemented to ensure effective oversight.

    1.3 Roles and responsibilities are well defined, documented, communicated, understood, and operating as intended.

2. Operational Readiness - Controls are in place and monitored to support cyber security operations.

    2.1 Incident management standard operating procedures/protocols exists and are operating effectively.

    2.2 Adequate resources and supporting technologies are in place to effectively respond to cyber security incidents.

    2.3 Security posture monitoring and reporting are conducted in a consistent, on-going manner, which informs and supports decision-making processes.

3. Risks, Dependencies and Inter-Dependencies - The IMITD understands its cyber security risks to operations and business processes.

    3.1 IMITD understands the cyber security risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

    3.2 IMITD's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

**Intent of this engagement's criteria and sub-criteria**

They establish the standards of performance and control against which performance will be assessed.

The assessment of performance compared to the expectations set out by the criteria will form the basis of audit findings.

These criteria and sub-criteria were developed specifically for this internal audit and are sourced from key directives, guidelines and standards identified within the 'Background' section of this document.