Environment and Climate Change Canada | Environnement et Changement climatique Canada

Canada

Audit of Cyber Security at Environment and Climate Change Canada (ECCC)

Final Report

AEB DGAÉ

Audit and Evaluation Branch

Direction générale de l'audit et de l'évaluation

Cat. No.: En4-760/2025E-PDF
ISBN: 978-0-660-75182-5
EC ID: 24013.13

Environment and Climate Change Canada
Public Information Centre
Place Vincent Massey building
351 St-Joseph boulevard
Gatineau Quebec K1A 0H3
Toll free: 1-800-668-6767
Email: enviroinfo@ec.gc.ca

Aussi disponible en français

Table of Contents

Background

Policy Framework

Cyber security is a shared responsibility across the Government of Canada (GC). While individual departments are responsible and accountable for the security of their endpoints and applications, other departments and agencies carry out specific government-wide responsibilities and provide advice and services to ECCC. Cyber security is the protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information. It includes the body of technologies, processes, practices and response and mitigation measures designed to protect networks, computers, programs and data from attack, damage, or unauthorized access to ensure confidentiality, integrity, and availability.

The Policy on Service and Digital and Directive on Service and Digital establish an enterprise-wide approach to the governance, planning, and management of cyber security. Among other requirements, deputy heads are responsible for ensuring that governance, planning, reporting, innovation and experimentation, and IT and information standards, are in place for a client and service delivery-focused model.

The Policy and Directive also stipulate that the Designated Official for Cyber Security, in collaboration with the departmental Chief Information Officer and Chief Security Officer as appropriate, is responsible for ensuring that cyber security requirements and appropriate risk-based measures are applied in accordance with the Directive on Security Management, Appendix B: Mandatory Procedures for Information Technology Security Control. These must be applied continuously, in an identify, protect, detect, respond, and recover approach to protect information systems and services.

Cyber Security at ECCC

As a science-driven department, ECCC depends on a wide array of applications, networks, and systems to fulfill its responsibilities. It handles and stores sensitive information concerning environmental policy, regulatory matters, and enforcement activities. Additionally, ECCC safeguards over a century's worth of meteorological data. Any theft or compromise of this data by malicious actors could jeopardize Canada's international competitiveness and economic interests, hinder innovation, and potentially threaten national security. Robust cyber security measures are essential to mitigating these risks.

The Department's Designated Official for Cyber Security is the Director General of Digital, Client, and Cyber Security Directorate in the Digital Services Branch, providing leadership and oversight of cyber security, in support to the departmental Chief Security Officer and the Chief

Service and Digital Officer. The Information Technology Security Management Division in the Digital Services Branch is responsible for managing the departmental cyber security function. The Division ensures that security requirements and appropriate risk-based measures are applied continuously in an identify, protect, detect, respond, and recover approach to safeguard ECCC's digital assets. The IT Security Management Division is supported by many key stakeholders and teams within the Digital Services Branch, who play a role in cyber security - the Service Desk, Cloud Centre of Expertise, the Web Application and Infrastructure Security Team, IT Desktop Engineering, Development, Business Applications and Solutions, Digital Transformation, Partnerships, Planning and Digital Resource Management, Data Analytics Services, Service Management, and Digital Products, Lifecycle Management and Telecommunications divisions.

Other stakeholders outside of the Digital Services Branch are responsible for risk-management activities in support of cyber-security - for example, the public Affairs and Communications Branch is responsible for the conduct of Privacy Impact Assessments, and the responsibility over business continuity plans falls under the Departmental Security Division in the Corporate Services and Finance Branch.

Objective, scope, and methodology

Objective

The audit objective was to assess the extent to which ECCC has an effective management control framework in place to meet policy requirements, identify vulnerabilities and incidents, and mitigate risks related to cyber security.

Scope

The audit scope focused on cyber security activities under the responsibility of ECCC and related to the corporate network (endpoints and applications), aiming to provide insights into the scale and scope of cyber risk management activities across the Department. The scope included an examination of select aspects within the Department's cyber security framework, based on the results of the risk assessment performed during the planning phase of the audit:

- Identification and management of risks, including governance of cyber security activities and risk assessment processes (i.e. security assessments, Privacy Impact Assessments, Business Impact Assessments, Threat and Risk Assessments) on information systems and digital assets deployed in its environment, including its application to local user systems)

- Implementation of protection measures to reduce risks, including cyber security awareness and training, and implementation of protective technologies (i.e. tracking of user-installed software)
- Monitoring, detection and understanding of cyber security events, which includes the continuous security monitoring of information systems and assets, and corrective actions upon detection

The scope excluded the review of cyber security controls impacting ECCC, but outside of ECCC's purview (i.e. cyber security controls managed by Shared Services Canada).

The period under review for the audit was April 1, 2022, to December 31, 2023.

Methodology

The audit was conducted and completed using the following methods:

- reviewing applicable TBS and departmental policy instruments and procedures for the management and administration of the IT security function
- conducted 65 interviews and walkthroughs with key personnel involved in the management of IT security and related activities, including site visits to more than 30 science facilities in 13 regional offices across the country
- mapping out the end-to-end processes related to areas under review and validating these processes with stakeholders to aid in identifying potential gaps and areas of improvement
- testing a randomly selected sample of 34 cyber security incidents across four sources, and a random sample of 10 Security Authorizations and Assessments
- testing and review of a sample of IT systems and supporting infrastructure (i.e. laboratories) to validate adherence to applicable standards. This includes systems managed under the Digital Services Branch as well as systems managed directly within branches

Statement of conformance

The audit conforms to the International Standards for the Professional Practice of Internal Auditing, as supported by the results of the quality assurance and improvement program.

Observations

Audit observations were developed through a process of comparing criteria (the correct state) with condition (the current state). Audit observations noted satisfactory performance, where the condition meets the criteria, or they may note areas for improvement, where there was a difference between the condition and the criteria. Where applicable, recommendations were made regarding conditions that were noted as areas of improvement. An overall audit conclusion was also made against the audit objective.

The observations, recommendations, and conclusion of this internal audit engagement were reported to senior management and the ECCC Departmental Audit Committee.

Management Response

Management agrees with the findings and accepts the recommendations of this internal audit. Where applicable, the Digital Services Branch has developed action plans to address findings and recommendations, the implementation of which will be monitored by the Audit and Evaluation Branch.

ECCC is committed to ensuring that the key control activities to mitigate cyber security risks are designed, implemented, and operating as intended.

Lines of enquiry and criteria

The following criteria were developed to address the objectives of the audit.

Line of enquiry 1: Cyber security governance, training and awareness

1.1 ECCC's cyber security governance and management policies and processes are established, with clear roles and responsibilities. This includes the role of the Designated Official for Cyber Security in providing leadership and oversight of cyber security, supporting the Chief Services and Digital Officer and the Chief Security Officer.

1.2 Cyber security training and awareness materials have been developed, communicated, and are accessible to employees.

1.3 Cyber security training activities are prepared and delivered on a regular basis to key departmental personnel involved in the application and maintenance of cyber security.

Line of enquiry 2: Cyber security in risk assessment and management

2.1 The Department has developed and communicated a security assessment (e.g. Privacy Impact Assessment, Business Impact Assessment, Threat and Risk Assessment) and authorization policy and procedures to facilitate the implementation of the policy and associated security controls.

2.2 The Department assesses the security controls in the information system and its environment of operation on a risk-based approach to determine the extent to which the controls are implemented correctly and meet established security requirements.

Line of enquiry 3: Implementation of protective measures to reduce risks

3.1 The Department has established policies governing the development, installation, and use of software by users and monitors and enforces compliance with these policies.

3.2 Controls are in place (e.g. access controls, privileged status, etc.) for the development, installation, and use and management of user-installed software.

3.3 The Department takes pre-emptive, reactive and corrective actions to remediate deficiencies and ensure that IT security practices and controls continue to meet the needs of the department.

Line of enquiry 4: Monitoring and reporting of cyber security threats

4.1 The Department has implemented the processes and technical tools to monitor, detect and report on abnormalities and incidents at application and endpoint level.

4.2 The Department performs monitoring and reporting and reviews the results of system monitoring,