Management Response and Action Plan - Audit of Cyber Security at Health Canada and the Public Health Agency of Canada

Recommendation 1

It is recommended that the ADM of DTB, who is the Designated Official for Cyber Security, in collaboration with the CIO and the ADM of CSB, who is also the CSO, review, update, document, and communicate the existing cyber security governance structure and committees to reflect the new DTB-CSB operating context, and to ensure that senior management is kept informed of potential and evolving cyber security issues, risk management practices, and performance metrics. These, in turn, will enable them to make informed decisions and provide strategic direction on how to mitigate anticipated cyber security related issues.

Management response

Management agrees with the recommendation.

Planned management action	Deliverables	Expected completion date	Responsibility
DTB (CIO) will collaborate with CSB (DCSO) to clarify accountabilities and support the development of a governance structure that reflects the roles of each branch, in alignment with the Departmental Security Plan (DSP), the Corporate Risk Profile (CRP) and relevant Treasury Board instruments, such as the *Directive on Service and Digital*.	1.1 An updated governance structure will be established and communicated to senior management for cyber security, including CSO, DOCS, CIO and other relevant stakeholders.	Q4 2023-24	DTB, with support from CSB (DCSO)

Planned management action	Deliverables	Expected completion date	Responsibility
DTB and CSB will inform senior management of security issues and risk management practices.	1.2 Following the formalization of a governance structure, a cyber security report will be developed and shared on a quarterly basis with the updated security governance structure and senior management. Reporting will leverage the data captured in the tracking tool noted in deliverable 2.1.	Q2 2024-25	DTB, with support from CSB (DCSO)

Recommendation 2

It is recommended that the ADM of DTB, in collaboration with the CIO and the ADM of CSB, implement a centralized system for tracking, prioritizing, monitoring and reporting on cyber security risks by capturing risks from internal processes, such as SA&As, trends identified by the Canadian Centre for Cyber Security and risks from government-wide monitoring.

Management response

Management agrees with the recommendation.

Planned management action	Deliverables	Expected completion date	Responsibility
DTB (CIO), with CSB's (DCSO) support will implement cyber security risk tracking, based on the CRP.	2.1 Establish a centralized tool for tracking, prioritizing, monitoring and reporting cyber security risks. This tool will be updated on a quarterly basis with reporting as outlined in deliverable 1.2	Q2 2024-25	DTB, with support from CSB (DCSO)

Date modified:
2024-04-16