Winnipeg | Audit

Cybersecurity Audit

May 2023

Leaders in building public trust in civic government.

Table of Contents

Audit Background

The intent of the audit is to:

Assess the state of the City's cybersecurity program as managed by the Innovation and Technology Department (IT), as well as the state of cybersecurity processes and controls for two (2) additional City IT divisions. The Audit Methodology is located in Appendix 1.

This audit assessed the City's documents, policies, practices, standards, processes and procedures to manage, monitor, and report on the organization's cybersecurity risks utilizing key functions of the National Institute Standards and Technology (NIST) Cyber Security Framework (CSF) (See Appendix 2) specific to the Detect, Respond and Recover domains.

Audit Objectives

The objective of this audit was:

To determine if the City has designed and implemented cybersecurity controls to manage, monitor and report on the organization's cybersecurity risks specific to their ability to detect, respond and recover from cybersecurity events, incidents and breaches.

Conclusion

The audit found that in several areas IT management is improving the City's overarching cybersecurity and cyber resiliency posture. A total of 25 recommendations spanning the four cybersecurity domains were made to improve the City's cybersecurity program. The confidential internal audit report outlines the detailed observations and recommendations.

Independence

The Audit Department team members and the external contractor selected for the audit did not have any conflict of interest related to the audit's subject matter.

Acknowledgement

The Audit Department and the external contractor extend their appreciation to all of the stakeholders who participated in this audit.

Jason Egert, Date: May 2023

Acting City Auditor

Overview

1.1 Background

- Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks. Also known as information technology security, cybersecurity measures are designed to combat threats against networked systems and applications, whether those threats originate from inside or outside of an organization.
- Cyberattacks are widely considered to be one of the most critical operational risks facing organizations. Cybersecurity threats are constantly evolving and becoming more sophisticated. With increasing numbers of cyberattacks, in particular ransomware, all types of private and public organizations must ensure they are prepared to ensure critical systems and services are restored.
- According to the *National Cyber Threat Assessment 2023 – 2024,* there has been an increase in threat activity against municipal and provincial governments. The Cyber Centre is aware of over 100 cases of cyber threat activity targeting Canadian municipalities since the beginning of 2020[1]. It is estimated that the average cost of a data breach, a compromise that includes but is not limited to ransomware, is $6.35 million[2].
- Proper management of a cybersecurity program is important to maintaining critical operations and services, while also protecting the confidentiality and integrity of sensitive data.

1.2 Reason for Confidential Report

- A confidential internal audit report was provided to the City's Audit Department and the IT Department. The report contains sensitive information, which if disclosed, could reasonably be expected to impact the safety and security of the City and its services.

[1] Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023-2024,* (2022).
[2] Canadian Centre for Cyber Security, *Cyber Threat Bulletin: The Ransomware Threat in 2021,* (November 2021).

Findings

The audit found that in several areas IT management is improving the City's overarching cybersecurity and cyber resiliency posture. These areas include:

- Key cybersecurity governance structures that will align security requirements, standards, and processes across the IT Department and the City's IT Divisions;
- New cyber incident response plan designed to provide repeatable processes for responding to cybersecurity incidents; and
- Key requirements and processes to standardize/align business continuity planning and recovery activities across City departments.

The confidential internal audit report outlines the detailed observations and recommendations to improve the City's cybersecurity program. The recommendations spanned across the following four cybersecurity domains:

- Governance - Five recommendations;
- Detect - Eight recommendations;
- Respond - Seven recommendations; and
- Recover - Five recommendations.

We encourage the City's IT management team to continue implementing their key cybersecurity initiatives, while actioning the recommendations presented in the confidential internal audit report.

Appendix 1 – Audit Methodology

The City Auditor is a statutory officer appointed by City Council under *The City of Winnipeg Charter*. The City Auditor is independent of the Public Service and reports directly to Executive Policy Committee, which serves as the City's Audit Committee.

The City Auditor conducts examinations of the operations of the City and its affiliated bodies to assist Council in its governance role of ensuring the Public Service's accountability for the quality of stewardship over public funds and for the achievement of value for money in City operations.

Once an audit report has been communicated to Council, it becomes a public document.

Project Risk Analysis

This audit was conducted using a risk-based methodology. A risk assessment was performed to identify the areas of focus for this audit.

Scope

The scope included the IT Department and two (2) additional IT Divisions. The procedures performed included interviews and control walkthroughs with key stakeholders, observation where necessary, and review of existing documents.

The scope for this engagement did not include:

- Assessment of any Departments/IT Divisions outside of the two divisions selected.
- Assessment of the operating effectiveness of the City's cybersecurity controls.

Approach and Criteria

This Cybersecurity Audit was conducted by an external contractor due to their expertise in cybersecurity and the skill set required to conduct the audit.

The audit was performed in accordance with Generally Accepted Auditing Standards (GAAS). Those standards require that the audit is planned and performed to obtain sufficient appropriate evidence to provide a reasonable basis for the observations and conclusions, based on the audit objectives.

The Audit criteria (elements of security Governance, Detect, Respond, and Recover from the NIST CSF) were identified and selected based on discussions with Innovation and Technology stakeholders, an assessment of key cybersecurity threats to municipalities and the core security capabilities for threat mitigation, as well as a risk assessment to help identify areas of

focus. An assessment of the NIST Identify and Protect domains was not included in the scope of work. The assessment of these criteria primarily focused on the design and implementation of the cybersecurity controls and their centralized delivery to the additional in-scope City Departments.

Appendix 2 – National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

The NIST CSF is a voluntary framework that outlines best practices to enhance cybersecurity protection. The NIST CSF was developed by the National Institute of Standards and Technology at the U.S. Department of Commerce, through on-going engagement and input from stakeholders in government, industry, and academia[3].

The framework aims to reduce and better manage cybersecurity risk and help organizations begin or improve their cybersecurity program. The following table outlines the core functions of the NIST CSF.

Function	Objective
Identify	Develop an organizational understanding to manage cybersecurity risk to: systems, assets, data, and capabilities
Protect	Develop and implement the appropriate safeguards to ensure delivery of services.
Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Source: https://www.nist.gov/cyberframework/framework

[3] National Institute of Standards and Technology. (March 2023). *History and Creation of the Framework.* https://www.nist.gov/cyberframework/online-learning/history-and-creation-framework