Office of the Auditor General
City of Hamilton

Cyber Security Follow Up Audit - Planning Summary – Public Report

April 10, 2025

Brigitte Minard, Deputy Auditor General
Charles Brown, Auditor General

Contents

Executive Summary

1 Cyber security refers to the policies, procedures, practices, and technology tools that collectively ensure electronic systems and data are protected from outside intrusion, tampering, theft, disruption, manipulation or loss. Poor cyber security practices or inadequate safeguards can lead to breaches of privacy, disclosures of confidential information, service outages, system shutdowns, operational impairments, loss of citizen confidence and legal liability, not to mention the high costs of recovering systems to normal.

2 The OAG conducted a Cyber Security Audit that was issued in April 2021 and made 29 confidential recommendations. The audit results were presented in closed session to Audit, Finance and Administration Committee.

3 The original Cyber Security Audit identified many serious issues, including a number of technical vulnerabilities. The OAG team included experts in cybersecurity who recommended a continuous improvement in security controls, a comprehensive plan to address vulnerabilities, and ongoing implementation and monitoring of the recommendations in their technical report.

4 The Office of the Auditor General typically completes a follow-up of major audits approximately 36 months after the original audit was issued, in order to provide sufficient time for major system and transformational changes to occur.

5 Report AUD21004 Cyber Security Audit was originally issued in April 2021, and a follow up was planned for the second half of 2024. However, the City of Hamilton experienced a major cyber security incident (a ransomware attack) in late February 2024. This presented an unprecedented situation in which a major security incident occurred prior to our second audit to follow-up on actions taken from the first audit. The intensity of efforts devoted to dealing with the incident and its recovery forestalled the OAG’s plans to conduct a follow-up. The incident has also prompted OAG to take a more in-depth approach to the follow-up, including a wider scope that examines the causes of the incident, the response of the City, and the adequacy of plans to prevent or minimize the risk further occurrences that would involve such profound effect.

6 In August 2024, as the cyber security incident response moved into the “Recover” phase, the OAG began the planning phase of the Cyber Security Follow Up Audit. The OAG engaged Valencia Risk to provide independent, expert, confidential advice to our Office. Valencia provided confidential, independent advice for the original Cyber Security Audit in 2021.

7 As of early 2025, the research and planning phase of the follow up audit has been completed and will be moving into the fieldwork phase. The OAG will report to the Audit, Finance and Administration Committee on the status of actions taken in response to the audit, and the Cyber attack, and OAG will independently evaluate the adequacy of its current plans, strategies, and cyber risk exposure with

recommendations for improvement. It is also the intention of OAG to conduct periodic audits of the implementation of the City’s response plan to the incident – referred to as a Roadmap, and to evaluate related cost forecasts.

2021 Cyber Security Audit - Summary

8 In 2021, the Office of Auditor General (OAG) took a holistic approach to evaluating the City’s cyber risks by looking at many facets important to IT security. The audit incorporated a comprehensive testing strategy involving two major components – assessment of risk exposures using recognized frameworks (Path to Enterprise Security, CIS Controls, CCCs (Canadian Centre for Cyber Security) Top Ten IT Security Actions and the NIST Framework. We also reviewed the IT security organization and strategic profile and had technical testing performed by outside experts (vulnerability assessments and penetration testing). Technical testing and evaluation conducted by the Office of the Auditor General team was supplemented with specialty technical expertise obtained from an external firm, Valencia Risk (Valencia).

9 IT is complex and requires the successful coordination of people, processes, planning, and governance. Our audit report contained findings and recommendations for all four of these areas.

10 To provide structure for this audit and to allow an overall assessment of the state of maturity of IT security, OAG used a tool created by the Canadian Centre for Cyber Security, an organization created by the Federal Government to provide a single, unified source of expert cyber security advice and guidance. The tool called “The Path to Enterprise Security” provides a framework for organizations to move their security protocols to appropriate levels of maturity. The maturity framework has five levels, each with their own criteria.

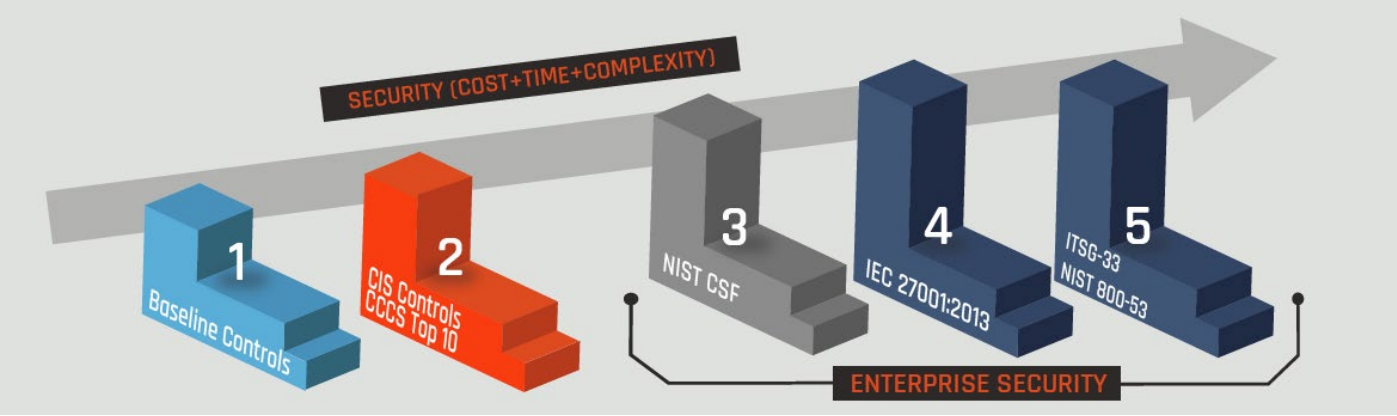


Image “The Path to Enterprise Security” from: https://www.cyber.gc.ca/en/path-enterprise-security

Criteria for Each Level

Level 1 - Baseline Controls

11 Designed to provide a balance between investment costs and cyber security outcomes.

Level 2 - Additional Controls/Actions

12 Looks at the deployment of measures beyond baseline controls:

a) The Center for Internet Security (CIS) Controls, available at https://www.cisecurity.org/controls/cis-controls-list/ were a set of 20 best practices recommended by the Centre for Internet Security based on known cyber attacks, since our audit in 2021, this as been renamed to the CIS Critical Security Controls, consisting of 18 critical security controls.

b) CCCS Top 10 IT Security Actions, is a list of 10 actions recommended by the Canadian Centre for Cyber Security (CCSC) to build a strong IT infrastructure and protect IT networks.

Level 3 - NIST Cyber Security Framework (CSF)

13 Consists of standards, guidelines, and best practices for managing cyber security risks through a cost-effective approach. The CSF is widely adopted in industry, and there are many sources for consulting, training, and implementing this framework. Since our audit in 2021, the NIST 2.0 Framework has been released, adding “governance” as a core framework component.

Level 4 - IEC 27001:2013 (now 27001:2022)

14 The international standard for cyber security. There is an industry related to the implementation and certification to this standard. An organization should consult ISO 27001:2013 or 27001:2022 if seeking certifications.

Level 5 - ITSG-33

15 National standards for cyber security ITSG-33 is the Government of Canada’s baseline advice and guidance for IT security risk management. This is the foundational enterprise security guidance.

16 OAG conducted its evaluation mainly at level 3 with some consideration of the degree of achievement of levels 1 and 2 protocols.

17 To provide assurance as to the achievement of Level 3, which was the level the OAG focused on primarily, the NIST Cyber Security Framework (CSF) was utilized. The NIST framework was created through collaboration between government and industry and consists of standards, guidelines, and practices to reduce cyber risks to critical infrastructure through a cost-effective approach (when compared to other standards such as ISO and ITSG-33, etc.). The NIST Cyber Security Framework is widely adopted in industry (see Figure 1). Since our Cyber Security Audit was issued, the NIST 2.0 framework has been released, and is being utilized for our Cyber Security Follow Up Audit.

Figure 1: Original NIST Cybersecurity Framework

Identify - Identify what processes and assets need protection.

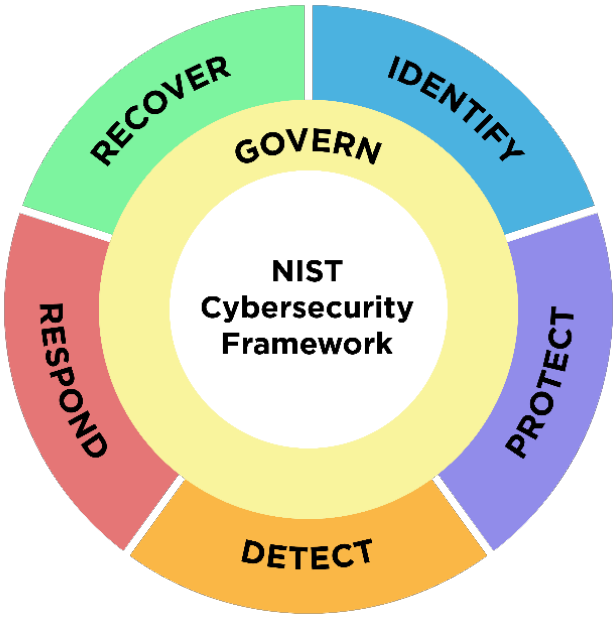
Protect - What safeguards are available.

Detect - What techniques can identify incidents.

Respond - What techniques can contain impact of incidents.

Recover - What techniques can restore capabilities.

Figure 2: NIST 2.0 Cybersecurity Framework



Govern – The organization’s cybersecurity risk management, strategy, expectations, and policy are established, communicated, and monitored.

Identify – The organization’s current cybersecurity risks are understood.

Protect – Safeguards to manage the organization’s cybersecurity risks are used.

Detect – Possible cybersecurity attacks and compromises are found and analyzed.

Respond – Actions regarding a detected cybersecurity incident are taken.

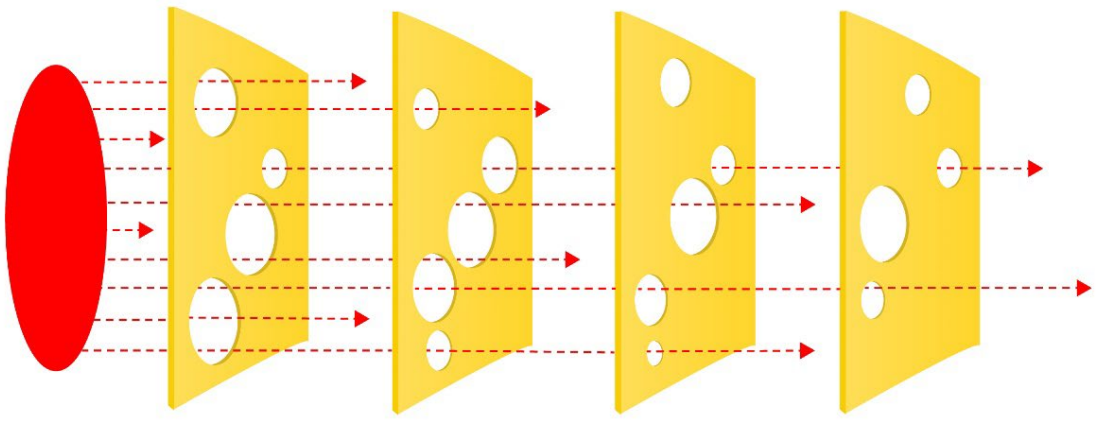
Recover – Assets and operations affected by a cybersecurity incident are restored.

Layered Security

18 Another important concept that was considered in the evaluation of IT security deployment is best described by the “Swiss Cheese Model” (Figure 3). The idea is that security measures should be built in layers so that a breach of one security protocol stands a good chance of being defeated by a second protocol. A strong program of security will be evidenced by these multiple layers stacked up like swiss cheese, where lapses and weaknesses in one defense do not allow a risk to materialize or “pass through the swiss cheese”, and a single point of failure is prevented by other layers.

19 What that means is the focus on cyber security efforts should not be limited to hardening the perimeter (the traditional thinking of IT security). It needs to be embedded into all areas of IT, so that that there are multiple layers of defense.

Figure 3 “Swiss Cheese Model”



2021 Cyber Security Audit Results

20 Overall, there were significant issues in all areas of the audit, and we grouped them into four main categories including:

- IT Processes and Operations
- IT Systems Planning and Recovery
- IT Authority and Governance
- People Matters

IT Processes and Operations

21 The OAG is unable to share technical findings and vulnerabilities related to IT Processes and Operations publicly, to maintain the safety and security of City assets. However, the results with respect to technical risks and vulnerabilities were reported to management and to Council in-camera.

IT Systems Planning and Recovery

22 Insofar as planning and recovery is concerned OAG found that the City needed to have a more comprehensive security planning process and a formal Cyber Security Plan. We also addressed the need for a systematic risk assessment process, more comprehensive monitoring, business continuity and recovery processes.

IT Authority and Governance

23 At the City of Hamilton, there have been efforts in the past few years to move towards IT centralization, however, there remain many decentralized elements to information technology in the organization, and barriers to integration, and the transition has been slow and difficult.

24 The IT Security Section in the IT Division managed cyber security risks that are within their span of control but can only indirectly manage security risks with systems not within their direct control. The Information Technology Division did not have authority for all things IT in the organization. This poses a significant and serious challenge for the management of cyber security risks. Further, as the IT landscape becomes more and more complex, it becomes even more of a challenge to effectively manage these risks.

People Matters

25 IT is complex, and the effective management of threats to IT requires the skill, awareness, training, vigilance, and commitment of people, including those who are not technically proficient in technology matters. When simulations are conducted to test employee responses to phishing attempts, the percentage of people that will respond to phishing spoofs by clicking on emails or giving their credentials has room for improvement.

26 Continued vigilance and senior leadership involvement in messaging the importance of protecting information and our vulnerability to outside attacks is crucial. Beyond this, we found that there was an opportunity to provide a broader set of training initiatives targeted toward senior leaders in the organization, or to those with key responsibilities for protecting IT assets or information and scaled or tailored to the important roles they play.

Overall Summary

27 Report AUD21004 included 29 confidential recommendations to improve cybersecurity at the City of Hamilton.

Cyber Security Follow Up Audit Scope and Objectives

28 The overall scope and objectives of this follow up audit are to:

- Review and compare the 2021 Cyber Security Audit findings (including the OAG’s NIST Framework assessment) with respect to weaknesses, risks, improvement opportunities and Assessment to those of the City of Hamilton’s Cybersecurity Consultants in their reports to management and Council to evaluate if meaningful progress was and is being made and whether certain OAG recommendations need to be reinforced, or new recommendations added.
- Determine if action and progress on the 2021 Cyber Security Audit recommendations was slow or inadequate, and if so, develop an understanding of the root contributing causes and possible solutions for more effective IT security governance.
- Analyze the City of Hamilton’s Cybersecurity Consultants reporting of the cyber-incident itself – its origins, causes and contributing factors.
- Assess the City of Hamilton’s Cybersecurity Consultant’s Proposed Road Map and the City’s Action Plan to:

- Identify any gaps or inadequacies in addressing OAG recommendations.
- Evaluate the adequacy and efficacy of the Road Map and City’s Action Plan in response to the cyber incident.
- Develop additional recommendations that the OAG believe to be prudent or necessary to augment or strengthen the Road Map, possibly including those beyond just technical controls such as governance, resources, long term strategies, risk management, organizational structure, best practices etc.

Next Steps

29 As of December 2024, the research and planning phase of the follow up audit has concluded and moved into the fieldwork phase in early 2025. The OAG will report the follow up audit findings to the Audit, Finance and Administration Committee when the follow up audit has concluded.

Office of the Auditor General
City of Hamilton

Charles Brown CPA, CA
Auditor General

Brigitte Minard CPA, CA, CIA, CGAP, CFE
Deputy Auditor General

Phone: 905-546-2424 ext. 2257
Email: auditorgeneral@hamilton.ca
Website: hamilton.ca/audit

SPEAK UP – Reporting Fraud and Waste

Online: Hamilton.ca/fraud

Phone: 1-888-390-0393

Mail: PO Box 91880, West Vancouver, BC V7V 4S4

Email: cityofhamilton@integritycounts.ca

Fax: 1-844-785-0699

Copies of our audit reports are available at: hamilton.ca/audit

Alternate report formats available upon request.