valencia

Ready for anything.

City of Hamilton
Elections Administration Audit
Technology Report

May 19, 2023

Table of Contents

1. Introduction
2. Audit Methodology
3. Summary
4. Findings & Recommendations
    a) Standards, Guidance, and Legislation
    b) Procurement
    c) Training and Support
    d) Project Management
    e) Controls

1. Introduction

The City of Hamilton engaged Valencia Risk to support the internal audit of IT controls surrounding the 2022 municipal election processes. Our objective was to examine and evaluate the use of technology and related administrative procedures and controls; specifically, the technologies used to maintain and administer the Voter's List; and the technologies used for Tabulation of the votes.

To do so, Valencia:

- Examined and evaluated IT systems, resources, vendors and vendor agreements as well as policies and procedures supporting electoral practices at the City and compliance with the Municipal Elections Act.
- Suggested actionable items based on recommendations to mitigate gaps in existing processes that can be implemented for the 2026 municipal election.
- Provided the Office of the Auditor General with suggestions for support or legislative reforms to be provided to the Province of Ontario through Elections Ontario.

2. Audit Methodology

In the absence of existing Canadian guidance or standards to assess electoral technical controls, Valencia has referenced the draft NIST Election Infrastructure Profile (NIST IR 8310) provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to election infrastructure.

Our team used this cybersecurity framework:

- To highlight and communicate high priority security expectations
- As a guideline for assessing the information gathered in interviews and in documentation to assess the state of City of Hamilton's elections technologies.

Emphasis was placed on six control categories from the NIST framework: Asset Management, Governance, Access Control, Awareness and Training, Anomalies and Events, and Recovery Planning.

These six controls categories were aligned, and high-level findings are summarized below.

3. Summary

Standards, Guidance, and Legislation

- Canadian standards have not been established for municipalities pertaining to technology and cybersecurity controls.
- Policies and procedures are based on prior years' elections processes and lessons learned.

Procurement

- Sole source for selection of DataFix (Voter's List) and Dominion (Vote Tabulator) was approved by Council, and relied on Elections Ontario own rigorous procurement practices and the US Election Assistance Commission Certification Process)
- Limited involvement of IT Department to establish technical security controls.
- No clear security requirements established in RFP or Contracts provided by Vendors.

Training and Support

- Training from DataFix and Dominion was limited to FAQ's and Online self serve with some "train the trainer" support.
- Staff training was not always mandatory and focused on execution and response to technical failures (manual processes established)
- Unclear engagement, roles and responsibilities regarding IT and IT Security.

3. Summary (continued)

Project Management

- Well organized and executed by Clerks office and IT project manager
- Limited number of continuing/experienced staff
- Reliance on past processes and lessons learned
- Well supported by Dominion
- Lack of support from DataFix (Specifically when troubleshooting electoral technologies)

Controls

- Standards and vendors used by the Province were adopted and adhered to by the Clerk's office
- Accountability for IT security and cybersecurity controls and standards was not well established or understood resulting in a complete reliance on contracted third parties.
- Weak controls regarding WiFi passwords for polling stations.
- Absence of Detective Intrusion Monitoring
- Assumptions made around detective controls to identify repeat/fictitious voters

Suggested support from Province and/or Legislative Reform

- Elections Ontario has established an Advisory Committee on Standards for Voting Technologies and will be taking over the voter's list from MPAC
- Request best practices for all municipalities that includes IT security standards

4. Findings

(a) Standards, Guidance, and Legislation

- We found no policies or procedure that specifically address cybersecurity for the election process.
- No Canadian Elections IT and cybersecurity standards currently exist. Valencia used the US NIST Framework on Cybersecurity (NIR 8310). It considers regulatory, risk, legal, environmental, operational controls.
- Cybersecurity expertise was not engaged internally or through a third party for the 2022 municipal election, leading to IT security roles and responsibilities not being fully defined.
- A risk assessment was completed; however, comprehensive IT threats, risks, and vulnerabilities were not documented, no cybersecurity personnel were involved in the election process.
- The Clerk's office addressed regulatory items, including civil liberties and privacy requirements.
- The IT department was not included in efforts to review IT configurations, assist with policy development, review of implementations, or to provide guidance on IT security.

Conclusion: Management is **compliant with established legislation** and **partially compliant** with the standards outlined in the Draft NIST IR 8310.

Recommendation: Until Canadian guidance is available, management should adopt the framework used in NIST IR 8310 and engage the IT department to ensure the skills required to address IT Security and Cybersecurity relevant to the Elections process.

4. Findings
(b) Procurement

- The Clerks office used sole sourcing to obtain elections technology and chose to use the same voting list (DataFix) and tabulation (Dominion) vendors. This was approved in advance by council.
- Hardware, rental inventory, and external information systems were thoroughly documented and catalogued; however, they were not prioritized based on classification, criteria, or business value.
- Cybersecurity expertise was not engaged internally or through a third party.
- The IT department was not fully engaged in the procurement process or finalization of contracts with DataFix or Dominion.
- Contracts were drafted by vendors and not by the City of Hamilton

Conclusion: Management is **compliant** for adherence to established internal policies and procedures. Management is **partially compliant** with standards outlined in the Draft NIST IR 8310.

Recommendation: Management should establish clear accountability for the IT department to prepare and review technology and IT security and cybersecurity requirements for both the RFP and the final contract.

4. Findings

(c) Training and Support

- Roles and responsibilities for technical team members in the context of the 2022 election were well understood and integrated in organizational charts.
- Delays at the polling stations were due to 2 main factors:
  1) Lack of Datafix server capacity for updates to the Voters' list
  2) Uncertainty at polling stations on when to transition to backup procedures to keep the voter line moving.
- Dominion Voting provided online and in-person training primarily director to senior individuals at the City of Hamilton.
- DataFix training was primarily provided online and through FAQ's and assistance was not timely when syncing issues delayed updates to the voter lists resulting in delays at some voting locations.

Conclusion: Management is **partially compliant** with the standards outlined in the Draft NIST IR 8310.

Recommendation: Management should make all training sessions mandatory for all staff involved in the elections process. The IT department should be invited to all training sessions. Training should be improved on when moving to backup processes.

4. Findings

(d) Project Management

- The Clerk's Office used project management effectively and engaged an IT project manager appropriately and showed maturity in its management of communications.
- Milestones, critical functions and dependencies for the 2022 elections were understood and established. Contingency planning included offline and/or manual backup to maintain the voter list and tabulation of votes. Load balancing was done on the website hosting the election results and select location testing to validate SIM cards connection prior to election day.
- A full understanding of the resilience requirements was achieved by the team; this did not translate into correct execution when server lag was experienced through DataFix.

Conclusion: Management is **compliant** with the standards outlined in the Draft NIST IR 8310 and established internal policies and procedures.

valencia

4. Findings

(e) Controls for Systems and Preparation

- IT systems for approximately 700 elections laptops, (ePollBooks) were configured, updated, and tested to the established specifications before the election.
- Despite the absence of cybersecurity guidelines, management developed appropriate and effective physical and IT security for election rooms, ballots, voter information, mail voting, information access, tabulators, regulators, and poll location Wi-Fi.
- The IT security team was short staffed. A cybersecurity team was not consistently engaged to identify, assess, or implement IT security technology; IT incident response and recovery plans were not developed or tested.
- An IT security vulnerability assessment, or management plan, specific to the elections process was not provided.

Conclusion: Management is **partially compliant** with the standards outlined in NIST IR 8310.

Recommendation: Management should complete an IT security vulnerability assessment and management plan specific to the Elections process.

valencia

4. Findings

(e) Controls for Risk Assessment

- A risk assessment was introduced and implemented for the first time in 2022.
- The City of Hamilton’s 2022 municipal election risk assessment concentrated on establishing a basic outline of potential threats with mitigation options, focusing on operational impact.
- Likelihood, impact, and mitigation strategies were identified, but did not factor in identified vulnerabilities or threats.
- Risk mitigation strategies and options were provided prior to the election. On election day, the City displayed good inventory capabilities for its physical devices and systems.

Conclusion: Management is **partially compliant** with the standards outlined in the Draft NIST IR 8310.

Recommendation: As a member of the Municipal Information Systems Association (MISA), Hamilton also has access to security threat feeds and resources. Management should consider an IT vulnerability assessment specific to external threats relevant to election day.

4. Findings

(e) Controls for Physical and Network Security

- Management used appropriate physical security and secure networks to protect data-at-rest.
- Data transitioned from polling locations to transmission sites was physically moved to a secure room for upload to a collator and sending to City Hall via a secure municipal network.
- Hardware inventory was maintained in Microsoft Excel sheets.
- Vote technologies used (DataFix and Dominion) were the same as used by Elections Ontario who required these vendors to provide proof of certification by the US Elections Assistance Commission. These technologies were also thoroughly tested by Elections Ontario.
- Reliance on e-mail "bcc" functionality for constituent communication contributed to a privacy breach.
- The City recorded a chain of custody for removable media such as memory cards and USD sticks used in the election. Items were protected by encoded zip-ties to ensure that potential tampering could be detected.
- Access to systems is controlled, with the technical team only having administrator privileges and only two people having access to election results folders.

Conclusion: Management is **compliant** with the applicable controls outlined in the NIST IR 8310.

4. Findings

(e) Controls for Access and Passwords

- Management documented and managed credentials and identities using a Contacts and Password List Excel spreadsheet.
- Some passwords were simple and easy to guess or crack.
- Knowledge of administrator credentials were held by technical team and election data folders had controlled read and write accesses (limited to 2 users).
- Physical access to assets was managed and protected by sealing memory cards with unique keys.
- Collation of election data took place on Hamilton laptops behind the DMZ to minimize risks and final reporting took place on a Dominion laptop never connected to the internet.

Conclusion: Management is **compliant** with the standards outlined in the Draft NIST IR 8310.

Recommendations: Management should consider improving password security by using passphrases or complex passwords. Municipal credentials would be stronger when paired with a password manager protected by multifactor authentication.

4. Findings

(e) Controls for Detection and Response

- Management did not deploy or test detection technologies specific to the 2022 municipal election (Cybersecurity detection requirements are not contemplated in current legislation).
- Management did not implement network monitoring, physical monitoring, or personnel monitoring for potential cybersecurity events.
- Detection methods were absent for mobile code, malicious code, and cybersecurity attacks.
- Monitoring processes for unauthorized personnel was limited and was absent for software or connection.
- Devices used for the 2022 elections were not assessed by an internal cybersecurity expert.
- Incident thresholds were not fully defined.
- No tabletop exercises were conducted to test IT incident response plans and contingencies.

Conclusion: Management has gaps in its detection methods regarding cybersecurity attacks and is **non-compliant** with the standards outlined in NIST IR 8310.

Recommendation: IT security should assess all devices and enable detection technologies specific to the Elections process and increase monitoring on election day.

4. Findings

(e) Controls for Incident Management

- A risk assessment was conducted prior to the election and included risk mitigation guidance.
- No IT incident response and recovery plans were identified specific to the election, however a lessons learned approach was taken by the City following the election highlighting issues and actionable items identified on election day.
- Technical teams were available, called upon to resolve ongoing issues.
- Immediate involvement of legal counsel and the privacy officer due to a privacy breach resulted from an error using the “bcc” function resulted in a successfully communicated and contained incident.
- In the case of delays in mail-in ballots, affected residents were contacted in a timely manner, open channels were there to communicate with City Hall about election issues.
- IT incident response plans specific to the Election were not developed or tested in advance.

Conclusion: Management is **partially compliant** with the standards outlined in the Draft NIST IR 8310.

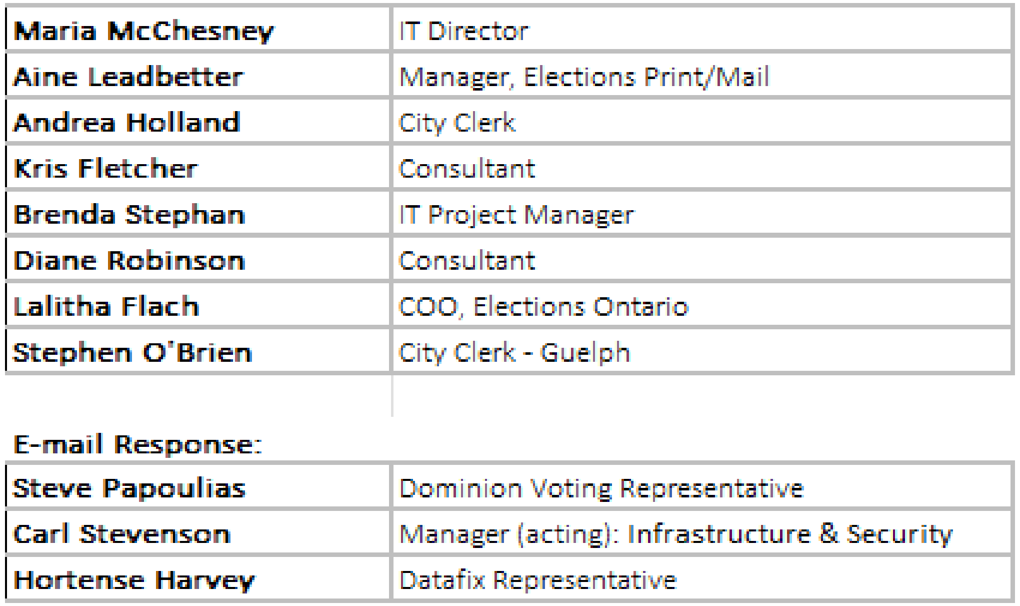
Recommendation: Management should consider use of technology appropriate for controlling distribution lists instead of relying on the “bcc” function. IT incident response scenarios should be developed and tested in a tabletop exercise.

Appendix

Documents Reviewed & Interviews

Documents: 245 documents were provided as support for Policies and Procedures referenced and developed for the 2022 election. 82 of these documents were considered in-scope for this internal audit.

Interviews:



Maria McChesney	IT Director
Aine Leadbetter	Manager, Elections Print/Mail
Andrea Holland	City Clerk
Kris Fletcher	Consultant
Brenda Stephan	IT Project Manager
Diane Robinson	Consultant
Lalitha Flach	COO, Elections Ontario
Stephen O'Brien	City Clerk - Guelph

E-mail Response:

Steve Papoulias	Dominion Voting Representative
Carl Stevenson	Manager (acting): Infrastructure & Security
Hortense Harvey	Datafix Representative

valencia

Ready for anything.

Prepared by Valencia IIP Advisors Ltd.

Our thanks to management who were responsive and transparent and have shown a clear desire for improvement by participating in this audit.