IT Asset Management 2024 Audit Report

October 7, 2024

Claire Mu, CIA, CISA, CPA, CFA, MMPA, MFin.
Director, Internal Audit

Richard Gervais, CISA, CISSP
Senior Advisor, IT Audit, Internal Audit

Balqees Omotosho, CISA, ISTQB
Senior Advisor, IT Audit, Internal Audit

Internal Audit

BRAMPTON

Table of Contents

Executive Summary

Background

The Information Technology (IT) Division, within the Corporate Support Services Department, is responsible for overseeing the IT asset lifecycle for the City of Brampton. This includes budgeting, procurement, deployment, maintenance, decommissioning, and disposal.

IT management advised the following: The division has been steadily building its IT asset management capabilities by implementing a centralized Configuration Management Database (CMDB) to track and manage assets, along with tools for network device discovery. Since 2023, efforts have focused on integration with other IT systems, including integrating mobile device management data, licensing, and IT contracts. Additionally, the process of asset purchases has been automated. These initiatives are part of an ongoing strategy to achieve a fully automated IT asset management system.

The IT Asset Management audit is part of the 2024 Internal Audit Work Plan, approved at the Audit Committee meeting held on February 13, 2024.

Audit Objectives

The IT asset management audit was conducted to assess the City's IT asset management policy framework, processes and practices, and tools for identifying, documenting, tracking, and monitoring hardware assets throughout their lifecycles.

What We Found

Areas of Strength

The Information Technology Division has established the technology infrastructure to manage IT assets. A key component of this infrastructure is CMDB. Automated tools that are integrated with the CMDB have been deployed to scan the network for network connected devices. The IT Division is actively working to enhance the automation of asset information collection from various data sources.

Summary of Findings

An IT asset management governance framework has not yet been established. There are no documented IT asset management policies, and standard operating procedures (SOPs) exist only in certain areas.

A governance framework should include a structured set of IT asset management policies, processes, standards, and practices. This will provide the necessary direction to effectively utilize the tools already in place, address the gaps highlighted in this audit and ensure IT asset management is effectively designed to support the City's business goals and objectives.

We identified that not all infrastructure devices have been entered into the CMDB Some of the devices reside in other systems that are in the process of being

integrated to the centralized CMDB. We also noted inconsistencies in the recorded data for existing devices.

Card access controls for locations housing critical IT assets are insufficient, as the current user access validation process fails to capture the complete list of active access cards. This gap presents a risk of unauthorized access to data centers.

There are no defined requirements for conducting pre-production or post-production testing. Management has stated that formal testing is intended to be part of the release management process. The release management process is still under development, and formalized testing procedures have not yet been fully established.

Finally, discrepancies were found in the documentation and oversight of IT asset disposals, raising concerns about the potential for improper handling of sensitive equipment and data.

Conclusion

We rated the audit as **Significant Improvement Required**. Although IT Division has established the technology infrastructure for managing IT assets, management has not yet implemented an IT asset governance framework. This governance would ensure consistent IT asset management practices across the division. Additionally, physical access to asset locations is a security matter and should be prioritized. Accurate accounting for IT assets in the IT asset disposal process should also be prioritized.

Although a documented IT change management process is in place, the process does not include explicit test requirements to ensure proper validation of changes. Formal testing procedures are part of the release management process, which is currently in development.

Addressing these issues will provide the direction and controls necessary to effectively leverage the existing IT asset management technology, strengthen asset security, and improve the CMDB's role in change management. Ultimately, this will ensure that the CMDB becomes the single source of truth for IT assets within the City of Brampton.

Thank You to Management and Staff

We appreciate the cooperation and assistance of the management and staff of the Information Technology, Corporate Security, Purchasing and Finance divisions during the audit.

Distribution List

Standard Recipients:
Members of Audit Committee

CAO

Members of Council

Members of Leadership Team (Division Heads and above)

KPMG LLP, Chartered Accountants (External Auditor)

Additional Recipients:
Information Technology Division

- Director, Technology and Cybersecurity
- Senior Manager, IT Client Services

Corporate Support Services:
- Director, Facilities Operations and Maintenance
- Senior Manager, Accounting Services & Deputy Treasurer

Public Works & Engineering
- Manager, Security Services
- Supervisor, Security Systems

Report Rating

Audit Report Rating

The report is rated:

- ○ Effective
- ○ Improvement Required
- ☑ Significant Improvement Required
- ○ Immediate Action Required

Background

The Information Technology Division plans, builds and sustains the City's digital, technology, and information environments to enhance service delivery. Their service commitments include maintaining 99.9 per cent network availability and resolving 61 per cent of incidents at first contact.

IT management advised the following: The division has been steadily building its IT asset management capabilities. The Service Desk Modernization Project, which ran from 2020 to the end of 2023, included the implementation of a centralized configuration management database (CMDB) to store and manage IT asset information, and eDiscovery which is a tool to scan the network for connected devices and import IT asset data into the CMDB. Further, since the end of 2023, the IT team has focused on fine-tuning the environment and driving continuous improvement through automation. This includes integrating Microsoft Intune (for managing mobile device data), Active Directory, licensing, and all IT contracts. The team has also streamlined the process of purchasing new equipment within the purchasing module of the City's financial application (PeopleSoft), ensuring that new assets are automatically entered into the system. This is an ongoing effort aimed at achieving a fully automated state.

The CMDB is designed to be the central source of accurate and comprehensive IT asset information for the City of Brampton.

IT Assets Definitions

For this audit, IT assets were defined as any information technology resource necessary to deliver IT services, including hardware, software, cloud services, and data.

The PeopleSoft application is used to track the monetary value of IT capital assets from their in-service date until they are fully depreciated. These assets are pooled and not tracked at the single device level in the accounting system.

Not all software and hardware IT assets used for service delivery are capitalized: for example, subscription-based software licenses are considered Project Operating Expenses. The City's *Tangible Capital Asset Accounting Standard Operating Procedure* sets a threshold of $1,000 for asset capitalization, with assets under this amount also capitalized if part of a larger project.

Capital and Operating Budgets

The following tables provide a breakdown of the IT capital and operating budgets in the context of the City's overall *2024 Budget*.

Table 1: IT Replacement Value and Capital Budget

Asset	City Total ($000s)	IT Total ($000s)	% of City Total
Asset Replacement Value 2023 (Excluding Land)[1]	9,000,000	162,000	1.8%
Asset Capital Budget 2024	545,630[2]	13,338[3]	2%

Table 2: The IT Operating and Capital Budgets as a Percentage of the Total City Budgets.

Operating	City Total Budget ($000s)	IT Budget ($000s)	% of Total Budget ($000s)
Total Operating	$912,578[4]	$37,597[5]	4%

Division of Responsibility related to IT Asset Management

IT Client Services

- IT Client Servicess oversees service delivery processes and supporting service delivery systems through the ITIL framework for Service Management including the IT Service Desk, Incident Management, Critical Incident Management and Change Management. The team also manages the Configuration Management Database, which serves as the repository for IT asset information.
- Additionally, IT Client Services oversees the End-User Computing refresh programs and manages all end-user-related assets within the CMDB.

IT Enterprise Systems

The IT Enterprise Systems team is responsible for the support and delivery of IT applications, ensuring effective procedures are in place for IT application management.

Technology and Cybersecurity

- The IT Security team reviews newly identified devices from the IT asset management process to ensure they pose no security risks.

[1] City of Brampton, *2024 Budget*, page 84
[2] City of Brampton, *2024 Budget*, page 104
[3] City of Brampton, *2024 Budget*, page 208
[4] City of Brampton, *2024 Budget*, page 35
[5] City of Brampton, *2024 Budget*, page 208

- The Architecture and Governance team is responsible for managing IT architecture and maintaining the Enterprise Architecture (EA) iServer solution, which lists IT software assets and cloud services. Planned integration between iServer and the CMDB will ensure that IT software assets identified by IT asset discovery tools are automatically pushed from the CMDB to keep iServer's inventory complete and up to date.
- The IT Infrastructure Services team focuses on managing the core IT infrastructure, including server, network and telecom systems, as well as data center operations. The team is responsible for managing IT infrastructure assets in the CMDB.

Supporting Corporate Support Processes

Purchasing manages the purchasing process per the By-law and establishes IT asset disposal services.

Finance tracks IT capital and operating asset spending via the PeopleSoft application and handles budget planning.

Security Services controls physical access to City of Brampton locations that house IT assets.

Key Process Areas

Identify and Record Current IT Assets

This foundational activity ensures an accurate, complete, and relevant IT asset database and includes:

- Identifying and recording IT assets with necessary details.
- Verifying IT assets to maintain a complete and accurate database.
- Recording IT asset values in the City's accounting systems.
- Controlling changes to IT assets through the IT Change Management Process.

IT Managers are responsible for the completeness and accuracy of IT asset information within their respective areas.

Identify and Manage Assets Essential for Supporting City Operations

This process aligns IT asset management with business requirements, providing management with information to manage IT assets and resources based on critical operational needs. The goal is to identify and maximize the reliability and availability of assets essential for IT service capability and City operations.

Business requirements and impact are considered when assessing the criticality of assets, including the impact of changes to assets, and when assessing incidents within the Incident Management process. This impact assessment determines the incident priority.

Manage the IT asset lifecycle

The IT asset lifecycle encompasses activities from asset planning to disposal. IT asset planning and purchasing must comply with Finance Division policies and the Purchasing By-law. Asset availability is maintained through incident management, monitoring, and preventative maintenance. Obsolete IT assets are securely retired and disposed of, with Security Services monitoring physical access to data centres, holding and storage locations. Table 3 describes the function of lifecycle activity as well as participants.

Table 3: IT Asset Management Lifecycle Activities and Responsible Parties

Lifecycle Activity	Departments/Divisions	Function
Planning	IT, Finance	Identify IT asset needs, create procurement plans and provide budgeting as well as forecasting information.
Procurement	IT, Purchasing, Finance	Identify requirements, select vendors, negotiate contracts and procure assets/services. Identify and record new IT assets. *
Deployment	IT, Facilities, Security Services	Install and configure assets, integrate new services, document details and secure areas. Update IT asset records.
Maintenance	IT, Security Services	Ensure performance, compliance and security, continuous monitoring, address issues. Access monitoring and reviews. Perform inventory counts. Maintain accurate IT asset records.
Decommissioning and Disposal	IT, Purchasing, Finance, Security Services	Responsible retirement, secure data removal, license deactivation and compliant disposal. Update IT asset records.

* The process of identifying and recording IT assets is performed as needed across the IT asset lifecycle.

IT Asset Management Audit History

The City of Brampton's Internal Audit Division has not conducted a comprehensive IT Asset Management audit. The 2020 IT Asset Management audit focused solely on End User Computing—specifically laptops and desktops—and the computer refresh program. The *2019 Data Centre* audit included the protection of IT assets within the data centre. Relevant findings from these audits were reviewed as part of this current audit.

Strengths	The Information Technology Division has established a technology infrastructure to manage IT assets as part of its modernization project. The goal is to establish the CMDB as the central source of accurate and comprehensive IT asset information for the City of Brampton.
IT Service Management	The IT division employs the Ivanti Service Management (ISM) suite of integrated products to manage IT service management activities. IT service management activities include but are not limited to, the Service Desk, incident and change management, and IT asset management.
Centralized IT Asset Data Repository	Consistent with industry best practices, the IT division has implemented a centralized IT asset data repository, known as a Configuration Management Database, as part of the ISM suite of tools. As a cloud-based SaaS (Software as a Service) solution, ISM ensures resilience, even if the City's IT infrastructure is compromised. ISM replaced the previous IT service management system, Helpdesk Expert Automation Tool (HEAT). The ISM CMDB eDiscovery began in June 2021.
Automated IT Asset Discovery	Automated IT asset discovery tools have been implemented to monitor the network for connected devices, aligning with industry best practices.
End User Computer Refresh Program	Laptops and desktop computers acquired through the End User Computer Refresh Program are recorded and tracked in the CMDB.
IT Capital Asset Management	The PeopleSoft application tracks the monetary value of capital IT assets until they are fully depreciated. The purchasing and finance accounting processes for acquiring and tracking the depreciation of IT capital assets are integrated, allowing information to flow from purchase requisition to the finance accounting system. The finance capital asset accounting and IT asset management are not integrated and are managed independently.

Audit Findings

A: An IT Asset Management Governance Framework Has Not Yet Been Established

Background The Information Technology Division has the technology infrastructure in place to manage IT assets. Consistent with industry best practices, the IT division has implemented a centralized IT asset data repository, known as a Configuration Management Database (CMDB), part of the ISM suite of tools. Automated IT asset discovery tools have been implemented to monitor the network for network-connected devices. IT assets are also identified through manual input, data import, and data synchronization. Updates to the CMDB are governed by the change management process. Laptops and desktop computers acquired through the End User Computer Refresh Program are recorded and tracked in the CMDB.

A1. There are Gaps in the IT Asset Management Policies and Procedures — Priority Rating P2

Criteria The City should establish IT asset management policies and procedures. These policies should be periodically reviewed and approved and should align with industry best practices and regulatory requirements.

Condition We observed and confirmed with management that there are no documented policies in place to govern IT asset management activities. Additionally, there are no SOPs in place for managing infrastructure and network IT assets. We reviewed existing IT asset management standard operating procedures used to manage end-user computer assets and noted they were outdated, contained obsolete information and lacked approvals and signoff.

As a result, we did not perform suitability or compliance testing of policies and operating procedures.

Impact The absence of IT asset management policies and standardized procedures across different IT teams has resulted in an incomplete and inaccurate CMDB and inconsistent IT asset information.

Documented policies and procedures are especially critical given the turnover in the Information Technology department, as they provide continuity and ensure consistent IT asset management practices despite personnel changes.

Without accurate data, tracking assets and auditing usage, ensuring compliance with licensing agreements can become challenging. It also limits the CMDB's integration with other IT service support processes, such as change management and undermines its reliability as the definitive source of authoritative source for IT assets in the City of Brampton.

A2. The IT Asset Database is Incomplete and Inconsistent **Priority Rating** **P2**

Criteria All IT asset data should be recorded in a centralized data repository to ensure a single authoritative source. IT asset discovery processes should be in place to ensure the completeness of the CMDB. Validation controls, including inventory checks should be implemented to ensure that records are accurate and up to date.

Condition Internal Audit did not conduct detailed analytics to test the completeness of the CMDB. Early in the process, we identified that further work is required by the Information Technology department to ensure the CMDB is complete, consistent and accurate. Testing for completeness and accuracy of the CMDB will be conducted in a future audit.

It was noted that the CMDB is not fully populated. During interviews with the Information Technology team, we learned that not all hardware assets have been recorded in the CMDB. Additionally, there are no inventory checks in place to validate the accuracy of the information. These issues have been attributed to the absence of synchronized discovery tools, the extensive manual effort required to update the CMDB and the limited size of the team.

We did note that IT asset information is not consistently recorded in the CMDB. There is no guideline specifying the minimum acceptable information that needs to be recorded for each asset in the CMDB.

Specifically, the review highlighted the following inconsistencies:

- 450 out of 451 production network switches have no location information.
- Of all 451 production network switches recorded in the CMDB, none had model information.
- 28 out of 718 production desktop computers had no location information.
- 4 out of 8 production wireless LAN controllers had no in-service date.
- 8 out of 8 production wireless LAN controllers had no location information.
- Of the 3 production routers recorded in the CMDB, none had device location, in-Service date and model information recorded.
- Of the 37 production firewalls recorded in the CMDB, none had model information recorded.
- Out of 47 production servers, none had location and model number information.

Impact An incomplete inventory of IT assets and inconsistency in recording asset information undermines the integrity and reliability of the CMDB as a comprehensive or authoritative source of asset information.

Recommendation:

1. **Implement an IT Asset Management Governance Framework**
   The Chief Information Officer should direct staff to implement an IT asset management governance framework with the goal of maintaining a complete, accurate and relevant Configuration Management Database that can be relied on as a comprehensive source of IT assets in support of IT service delivery and planning activities, and the framework, at a minimum should include the following elements:
   a. goals and objectives for IT asset management
   b. defined policies
   c. specified roles and responsibilities
   d. consistent and measurable standard operating procedures.

B: The Data Centre Card Access Review Process Does Not Capture All Active Access Cards

Background Access cards are required to gain physical access to data centres and other locations where IT infrastructure assets are located.

The Security Services Division in the Public Works Department manages the access card system and user accounts. The user access list is reviewed monthly with key stakeholders, including IT, to ensure only authorized users are granted access to those sensitive locations.

B1. The Data Centre Access Review Process Contains Inaccuracies — Priority Rating: P2

Criteria Physical access controls should be established to restrict entry to locations containing critical IT assets, ensuring that only authorized personnel have access. A formal user access provisioning process should be implemented to manage the addition and removal of user access, with periodic management reviews of access lists and logs by management. This ensures ongoing security, compliance, and timely detection of any unauthorized access.

Condition The current methodology to validate the user access list is not adequately capturing the full scope of active access cards. Specifically, the reviewer relies on a manually compiled list of "approved individuals" who should have access to the data centre.

However, this list is not cross-referenced with the access card management system, which is the authoritative source of access information.

A comparison between the system-generated access list and the manually maintained list revealed the following discrepancies:

- Multiple Cards Not Accounted For: Some individuals on the system-generated list have multiple access cards, but only one of their cards is recorded in the manual list.
- Incomplete Population: There are individuals on the system-generated list who are not included in the manually compiled list.

Impact There is the potential for unauthorized access to the data centres. The discrepancies noted indicate that the current review process does not accurately reflect the full population of individuals with access to the data centre.

Recommendation:

2. **Enhance the Card Access List Review Process**
   The Director, Facilities Operations & Maintenance, should direct staff to revise the data center access review process to include all active cards by using a system-generated access list, confirming custody of multiple cards, and deactivating unused cards.

C: The Change Management Process Guide Does Not Include a Formal Testing Requirement

Background Effective management of IT assets is crucial to the City's ability to deliver reliable and secure services. The Information Technology Division has implemented a Change Management Process Guide that governs the planning, assessment, and implementation of changes to IT assets. Changes are recorded in the IT Service Management tool.

C1. The Change Management Process Lacks Testing Requirements

Priority Rating **P2**

Criteria The City should establish a Change Management process that governs the planning, assessment, and implementation of changes to IT assets. Changes should be recorded in the IT Service Management tool with clear linkages to the assets recorded in the CMDB.

Condition The *Change Management Guide* does not include requirements for documenting evidence of testing. For 16 out of 25 sampled changes, including firewall configuration changes, server upgrades, and patching activities, no formal test documentation was included in the change ticket, nor was any rationale provided for the absence of testing. Internal Audit could not verify that testing was conducted to ensure the changes would not negatively impact the IT environment.

Management indicated changes are being tested but there is no requirement for implementors to attach test results to the change record. Although there was no evidence testing was performed, we noted that all 25 sample changes were successfully implemented.

We also observed that there are no defined requirements for conducting pre-production or post-production testing. Management has stated that formal testing is intended to be part of the release management process. However, the release management process is still under development, and formalized testing procedures have not yet been fully established.

Impact The absence of a testing requirement presents a risk to the stability and security of IT assets, as untested changes could result in system failures, security vulnerabilities, and potential disruptions to business operations.

Recommendation:

3. **Revise the *Change Management Process Guide***
   The Chief Information Officer should direct staff, until the release management process is implemented, to revise the *Change Management Process Guide* to ensure that it includes:

   a. requirements for documenting test procedures and results

   b. documentation of exceptions, such as when testing is not feasible.

D: The IT Asset Disposal Process is Inconsistent

Background In accordance with the City's asset disposal process, IT assets that have reached the end of their lifecycle are retired and disposed of through an electronic waste disposal vendor. The vendor is selected by following a competitive bidding process. The vendor assumes responsibility for securely erasing data on the devices and provides a "secure wipe" report to confirm that all information has been removed. Additionally, some network devices being retired are returned to the manufacturer as part of an exchange program for replacement. For any devices deemed salvageable, the vendor makes a purchase and remits payment to the Finance team.

D1. There are Gaps in the IT Asset Disposal Process — Priority Rating P3

Criteria The City should enforce a consistent procedure for the secure disposal of retired IT assets. This process should include obtaining a certificate of destruction from the recycling firm, maintaining a list of disposed IT assets, and ensuring secure pick-up and delivery of the assets.

Condition Discrepancies were identified in the documentation and oversight of asset disposals. Specifically:

- Discrepancies in Documentation:

  For three out of the six disposal approval forms that were reviewed, the number of assets documented in the disposal approval forms did not match the records in the disposal master sheet.

- Lack of Oversight in Approvals and Segregation of Duties:

  Two disposal forms with incorrect asset counts were approved, none of the approvers noted the discrepancies, indicating a lack of thorough review.

  Based on the information on the documents provided, it appears one individual was responsible for the end user computing disposal process from identification of end-of-life devices to dispatch to the disposal vendor.

- Inadequate Process Controls:

  The asset disposal forms are required to be approved by the CIO, the asset analyst's manager and a purchasing agent; four out of six disposal forms were missing some or in some cases all the required approvals.

- Inconsistent disposal practices:

  There are inconsistencies in the City's asset disposal process. The auditor noted instances where the disposal master sheet and asset disposal form were not completed/approved.

Impact

- Potential Financial Loss:

  There are potential costs associated with data or privacy breaches, regulatory fines, and legal actions.

  Please note that devices being decommissioned at end-of-life have no residual asset value.

Recommendation:

4. **Strengthen the IT Asset Disposal Process**
   The Chief Information Officer should direct staff to review and update the IT asset disposal process to ensure accurate completion of asset disposal forms with appropriate sign-off reviews.

Conclusion

Significant Improvement Required

Based on the overall findings, we have concluded that the audit warrants a rating of **Significant Improvement Required**.

We evaluated the City's IT asset management policies, processes, practices, and tools used to identify, document, track, and monitor hardware assets throughout their lifecycles.

The IT Division has built a technological foundation for IT asset management, with the Configuration Management Database (CMDB) serving as the central repository for managing these assets.

IT Asset Management Governance Framework

Maintaining a complete and accurate IT asset repository is a core objective of IT asset management. However, we found that the CMDB is incomplete, with inconsistencies in asset records. The absence of a comprehensive IT asset management governance framework is likely the primary cause of these discrepancies.

Four Key Findings

In summary, the four key findings are: the absence of an IT asset management governance framework, incomplete data centre card access reviews that do not account for all active access cards, lack of formal, documented requirements for mandatory testing and the attachment of test documentation for each change in the change management process, and inconsistencies in the IT asset disposal process.

Single Source of Truth

Addressing these issues will improve IT operations management, strengthen security, and ensure the CMDB becomes the single source of truth for IT assets in the City of Brampton.

Audit Objectives, Scope and Methodology

Objectives

The IT Asset Management (ITAM) audit is part of the 2024 Internal Audit Work Plan. The audit aims to evaluate the City's IT asset management framework, processes, and tools for identifying, documenting, tracking, and monitoring hardware assets throughout their lifecycles.

Specifically, the audit assessed the following components of IT Asset Management:

1. **IT Asset Inventory**: Assess the completeness and accuracy of the IT asset inventory as recorded in the Configuration Management Database.
2. **Critical Asset Controls**: Evaluate the effectiveness of controls in identifying critical IT assets essential for City service delivery.
3. **Change Management Process**: Assess the IT Change Management process to ensure that all changes to IT assets are documented, formally approved, effectively communicated, and accurately reflected in the CMDB.
4. **IT Asset Lifecycle Controls**: Assess the adequacy and effectiveness of controls over the IT asset lifecycle from procurement to disposal.
5. **Access Controls**: Assess whether access to the CMDB is restricted to authorized user and service accounts, consistent with their role in asset management.
6. **IT Capital Asset Financial Records**: Verify whether IT capital asset purchases are accurately recorded in the accounting system and that the depreciation of these IT assets is tracked through to their end-of-life. From the accounting perspective IT assets are disposed on the books when they are fully depreciated.
7. **Financial Accuracy for Budgeting:** Assess the completeness and accuracy of financial records of IT assets.
8. **Policies and Procedures**: Evaluate whether the IT asset management policies and procedures are adequate and up to date.
9. **Compliance with Policies and Procedures:** Assess the level of compliance with IT asset management policies and procedures.

Scope

The audit period covered IT asset management activities from June 1, 2021 to June 31, 2024.

IT assets in scope include:

- Any information technology hardware resources necessary for delivering IT services.
- All IT assets owned or managed by the IT Division.

Please note that the above scope does not preclude us from looking into any other areas that may come to our attention and warrant a review during the audit. If the scope of the audit is expanded, the audit committee will be informed.

Scope Exclusion

Mobile Phone Management: This area is not within the scope of this audit and will be addressed in future audit engagements.

IT Software and Cloud Asset License and Subscription Management: These areas are not within the scope of this audit and will be addressed in future audit engagements.

Methodology

We employed the following methodologies to ensure a thorough and effective review:

- Compiled a risk control matrix to help prioritize our audit review based on the identification of high-risk areas within IT asset management. This approach enabled us to concentrate our efforts on areas that have the greatest potential for impact.
- Interviewed key stakeholders during the planning and execution phases of the audit to obtain an understanding of IT asset management practices within the City.
- Conducted walkthroughs of the Configuration Management Database, IT assets management practices, data centre security, IT asset-related finance and purchasing processes.
- Reviewed policies and procedures related to the City's IT asset management life cycle and assessed compliance with these policies and procedures.
- Tested key controls associated with IT asset management and security to evaluate their effectiveness in mitigating identified risks and to confirm that they are functioning as intended.
- Performed analytics on the CMDB and access card report to identify inconsistencies.

Appendix 1: Management Response to the Audit Report

Recommendation 1: Implement an IT Asset Management Governance Framework

The Chief Information Officer should direct staff to implement an IT asset management governance framework with the goal of maintaining a complete, accurate and relevant Configuration Management Database that can be relied on as a comprehensive source of IT assets in support of IT service delivery and planning activities and the framework, at a minimum, should include the following elements:

a. goals and objectives for IT asset management
b. defined policies
c. specified roles and responsibilities
d. consistent and measurable standard operating procedures.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan

Comments:
We acknowledge the recommendation to implement an IT Asset Management (ITAM) strategy and agree on the importance of maintaining a complete, accurate, and reliable CMDB (Configuration Management Database) to support IT service delivery and planning activities. IT Assets with their required information are currently documented across three systems.

Internal Audit was advised that the IT Service Management team has already planned for and initiated a *CMDB Enhancement Project*, which preemptively addressed many of the IT audit findings, including the need for consolidation of asset data from these disparate systems into a centralized CMDB. IT is actively pursuing automation and integration efforts to ensure the accuracy and comprehensiveness of asset management.

Actions:
IT will continue with the existing workplan established prior to the audit, to implement the centralized, automated CMDB with an asset strategy, policies and processes within the established project timelines.

Timeline: December 2025

Recommendation 2: Enhance the Card Access List Review Process

The Director, Facilities Operations & Maintenance should direct staff to revise the data center access review process to include all active cards by using a system-generated access list, confirming custody of multiple cards and deactivating unused cards.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan

Security Services will generate a newly created automated monthly report for the Chief Information Officer. This report will include all access cards with access to any of the three data centres, including staff with multiple cards. The report will be sent to Security Services for cross-referencing access provisions.

Information Technology will be responsible for reviewing the monthly report and providing comments and updates. Once Security Services receives the comments and updates from Information Technology any applicable changes will be made.

The rebadging project scheduled for 2025 will remove users from having multiple cards.

Timeline: 1 October 2024

Recommendation 3: Revise the Change Management Process Guide

The Chief Information Officer should direct staff, until the release management process is implemented, to revise the *Change Management Process Guide* to ensure that it includes:

a. requirements for documenting test procedures and results

b. documentation of exceptions, such as when testing is not feasible.

Management Response: ☒ Agree ☐ Disagree

Comments/Action Plan

Comments:

While documented test results are not attached to each change, all changes except for those listed below do go through the Tricentis Suite of products for testing and quality assurance. Those results are recorded within the suite. In addition, Release Management processes will require testing results to be documented. Where non-production environments are unavailable, a validation process will be implemented. Testing and validation results will be required to be attached to each Change.

Our current Change Management Process is not only well-established, mature, and fully documented, but also aligns with industry best practices, including Information Technology Infrastructure Library (ITIL) standards. This robust process successfully manages and documents approximately 1,200 changes annually with a 97.5% successful implementation rate.

Actions: IT Service Management will adjust the process to make documented test results mandatory, which will include a link to the Tricentis Suite for test results and will continue to rollout Release Management as planned.

Timeline June 2025

Recommendation 4: Strengthen the IT Asset Disposal Process

The Chief Information Officer should direct staff to review and update the IT asset disposal process to ensure accurate completion of asset disposal forms with appropriate sign-off reviews.

Management Response: ☒ Agree ☐ Disagree
Comments/Action Plan Comments: Management agrees with the findings of this section of the audit. Actions: Information Technology will update the process to implement a mandatory reviewer and approver, as well as vendor compliance steps and align this process across the Division. **Timeline: December 2024**

Appendix 2: Criteria for Assigning a Rating to Audit Findings

Priority Rating	Description
Priority 1 (P1)	**One or more of the following conditions exist that require immediate attention of the Senior Leadership Team. Corrective actions by senior Management must be implemented.** • Financial impact of both actual and potential losses is material • Management's actions, or lack thereof, have resulted in the compromise of a key process or control, which requires immediate significant efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks. Failure by Management to remedy such deficiencies on a timely basis will result in the City being exposed to immediate risk and/or financial loss • One more of the following conditions is true: i) management failed to identify key risks, ii) management failed to implement process and controls to mitigate key risks • Management's actions, or lack thereof, have resulted in a key initiative to be significantly impacted or delayed, and the financial support for such initiative will likely be compromised • Management failed to implement effective control environment or provide adequate oversight, resulting in a negative pervasive impact on the City or potential fraudulent acts by City staff • Fraud by management or staff, as defined by the *Corporate Fraud Prevention Policy*.

Priority 2 (P2)	**One or more of the following conditions exist that require attention by senior Management. Corrective actions by management should be implemented.** • Financial impact of both actual and potential losses is significant • Management's actions, or lack thereof, may result in a key process or control to be compromised, which requires considerable efforts and/or resources (including time, financial commitments etc.) to mitigate associated risks • Management correctly identified key risks and have implemented processes and controls to mitigate such risks, however, one or more of the following is true: i) the processes and controls are not appropriate or adequate in design, ii) the processes and controls are not operating effectively on a consistent basis • Management's actions, or lack thereof, have impacted or delayed a key initiative, and the funding for such initiative may be compromised • Management failed to provide effective control environment or oversight on a consistent basis, resulting in a negative impact on the respective division, or other departments • Management failed to comply with Council-approved policies, by-laws, regulatory requirements, etc., which may result in penalties • Management failed to identify or remedy key control deficiencies that may impact the effectiveness of anti-fraud programs
Priority 3 (P3)	**One or more of the following conditions exist that require attention by management. Corrective actions by management should be implemented.** • Financial impact of both actual and potential losses is insignificant • A non-key process or control, if compromised, may require some efforts and/or resources (including time, financial commitments, etc.) to mitigate associated risks • Processes and controls to mitigate risks are in place; however, opportunities exist to further enhance the effectiveness or efficiency of such processes and controls. Management oversight exists to ensure key processes and controls are operating effectively • Minimal risk of non-compliance to Council-approved policies, by-laws, regulatory requirements, etc. • Low impact to the City's strategic or key initiative • Low impact to the City's operations

Appendix 3: Criteria for Assigning a Rating to Audit Reports

Rating	Description
Effective	• Key controls are adequately and appropriately designed, and are operating effectively to support objectives and manage risks • Audit recommendations resulted in only minor enhancements to the effectiveness or efficiency of controls and processes • One or more Priority 3 findings • Insignificant cumulative financial impact when all audit findings have been considered • Audit findings would not be subject to a follow-up by Internal Audit
Improvement Required	• A few control weaknesses were noted that require enhancements to better support objectives and manage risks • One Priority 2 and Priority 3 findings • Priority 3 findings only where the cumulative financial impact is significant • Corrective action and oversight by management is needed • Audit findings could be subject to a follow-up by Internal Audit
Significant Improvement Required	• Numerous key control weaknesses were noted that require significant improvement to support objectives and manage risks • One Priority 1 finding or more than one Priority 2 findings and Priority 3 findings • Priority 2 and 3 findings only where the cumulative financial impact is significant • Corrective action and oversight by senior Management is required • Audit findings will be subject to a follow-up by Internal Audit
Immediate Action Required	• Key controls are either not adequately or appropriately designed and are not operating effectively, or there is an absence of appropriate key controls to support objectives and manage risks • More than one Priority 1 finding, combined with Priority 2 or 3 findings • Regardless of the type of findings, the cumulative financial impact is material to the City's financial statements. • Confirmed fraud by management or staff • Corrective action and oversight by Senior Leadership Team is required immediately • Follow-up of such audit findings by Internal Audit would be of high priority


BRAMPTON