TECHNOLOGY CHANGE MANAGEMENT

PROGRAM EVALUATION AND AUDIT

METROPOLITAN COUNCIL

Contents

Highlights

The Council failed to develop formal policies, procedures, and standards for technology change management.

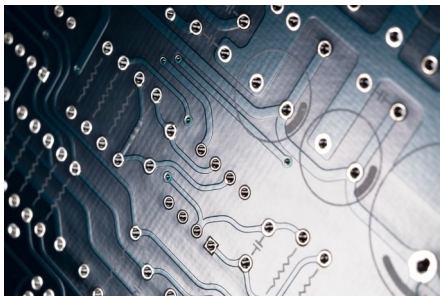
What We Found

What's Working Well

Metropolitan Council divisions and departments have implemented some processes for technology change management. The Change Advisory Board (CAB) is managed by the Information Services (IS) department and includes technicians and business process owners from across the Council. The CAB oversees some technology change management activities for the Council.

What Needs Improvement

The Council does not have policies, procedures, or standards for technology change management. The CAB is not charted and does not have formal authority or documented roles and responsibilities for technology asset and application change management. The IS Department and Council Divisions are not using industry best practices to inform controls and set standards to manage changes.



What We Recommend

The Regional Administrator should charter and assign authority with defined roles and responsibilities for the CAB. The Regional Administrator should commission and approve technology change management policies, procedures, and standards. Technology standards implemented should be informed by industry best practices.

Why We Did This Work

This audit evaluated the controls the Council has developed and implemented for technology change management, including controls implemented by the CAB and change activities managed outside the IS Department.

What We Reviewed

Audit reviewed technology change management activities from Regional Administration (RA), Environmental Services (ES), and Metro Transit (MT), along with CAB activities and processes managed by the IS Department and technicians in other Council Divisions.

How We Did This Work

Audit conducted interviews with the CAB and Council staff from IS, MT, and ES. Audit conducted interviews with Council staff and reviewed information regarding change management activities. The interviews covered technology general controls related to change management.

Summary of Findings

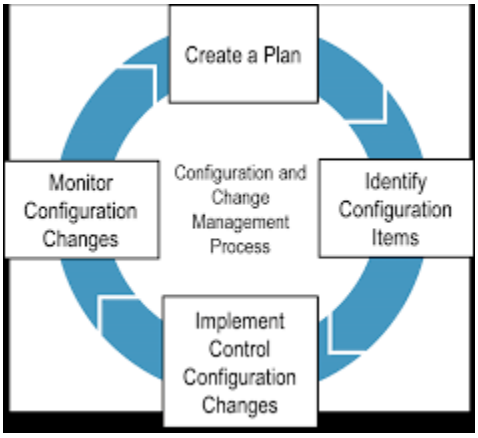
Number	Description	Recommendation	Follow-up Action	Page
Observation 1	The Council does not have technology change management policies, procedures, or standards.	The Regional Administrator should ensure that formal change management policies and procedures, and the required technology standards are developed based on industry best practices for the Council's divisions.	Confirmation	9
		The Regional Administrator should ensure procedures for change management outline the responsibility of the CAB within the procedure and standards based on industry best practices. Senior management should hold the divisions of the Council accountable for ensuring support and adoption of technology change management standards.	Confirmation	9
Observation 2	The CAB does not have formal authority, defined roles, or responsibilities for technology change management activities.	The Regional Administrator should formally charter and ensure the appropriate Sponsor(s) are established to ensure the CAB has the appropriate authority to oversee and recommend approval or rejections for changes for the Council.	Confirmation	10
		The Regional Administrator should ensure the CAB uses technology standards and industry best practices for change management, as mandated by the *Technology Governance Policy (TECH 1-2)* and the Council's Policy and Procedure Framework.	Confirmation	11

Introduction

Background

The National Institute of Standards and Technology (NIST) defines change management as "a collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle."[1] Such activities include having formal policies, procedures, and processes to manage information system changes. The technology change management process should be controlled and repeatable, ensuring segregation of duties through all phases of the change and appropriate change testing and approvals (Figure 1).

Figure 1: Change Management Lifecycle



From "CRR Supplemental Resource Guide, Volume 3: Configuration and Change Management" by CISA.gov (*CRR Supplemental Resource Guide, Volume 3: Configuration and Change Management (cisa.gov)*)

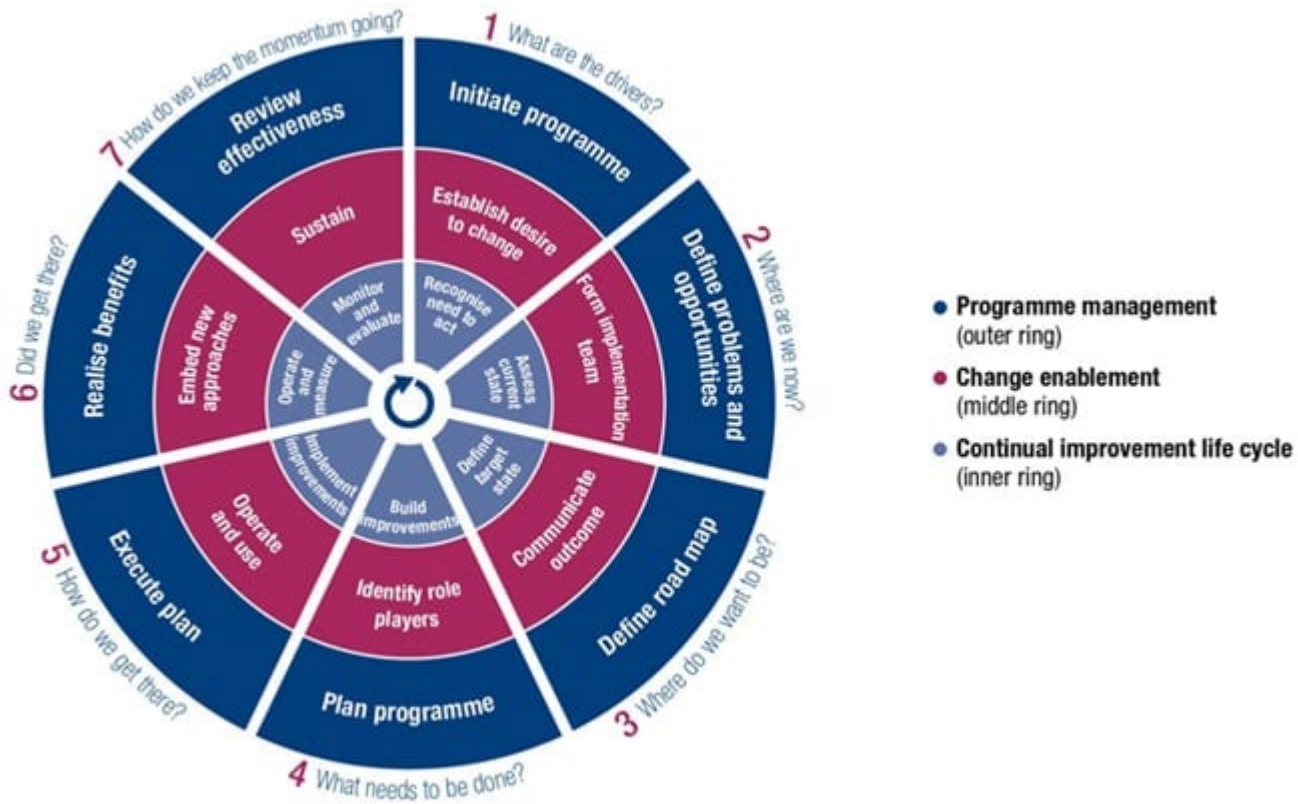
The Council's *Technology Governance Policy (TECH 1-2)* describes the functions of a technology governance framework and requires effective input and decision-making pertaining to technology principles, procedures, standards, and processes. The *Technology Governance Policy (TECH 1-2)* does not define an effective standard. However, the Council's Policy and Procedure Framework defines effective standards as being informed by industry best practices and linked to a control framework. NIST and Center for Internet Security (CIS) provide open-source guidance. NIST and CIS guidance cover the array of controls organizations should implement for information and cyber security, based on organization considerations and risk ratings. The Federal Transportation Authority has required organizations receiving FTA funds to self-certify they have a process that develops, maintains, and executes written plans for identify and reducing cybersecurity risks that uses NIST guidance. Additionally, Governor Walz issued Executive Order 22-20 "Directing State Agencies to

[1] NIST. (2022, January 19). *COMPUTER SECURITY RESOURCE CENTER*. NIST CSRC: https://csrc.nist.gov/glossary/term/cm_uppercase

Implement Cybersecurity Measures to Protect Critical Infrastructure in Minnesota. In response to this, the IS depart has decided the Council's technology standards should include CIS control guidance.

NIST recommends establishing Configuration Control Boards or CABs for managing configuration changes to systems. A formal CAB charter would include defined authority, purpose and objectives, deliverables, activities, and membership. Configuration change control for organizational systems involves the systematic proposal, justification, implementation, testing, review, and disposition of system changes, including system upgrades and modifications. NIST guidance states organizations should document the types of changes to the system, review proposed changes to the system, approve or disapprove changes, document configuration change decisions, and coordinate and provide oversight for configuration change control activities.[2] ISACA provides some context as to how the technology change management process can be enabled through the life cycle phases of information products and systems (Figure 2).

Figure 2: Change Enablement Life Cycle Phases



Change Enablement Life Cycle Phases Source: ISACA, *COBIT 5 Implementation*, 2012, p. 36

The IS Department has chosen to implement the CIS controls. Technology change management would be impacted by CIS Control 4 related to the *Secure Configuration of Enterprise Assets and Software*, states that an organization should establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-

[2] NIST. (2020, September). NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations. USA.

computing/IoT devices; and servers) and software (operating systems and applications).[3] Per CIS, even after a strong initial configuration is developed and applied, it must be continually managed to avoid degrading security as software is updated or patched, new security vulnerabilities are reported, and configurations are "tweaked."

Managed within IS, the CAB oversees some technology change management activities for the Council. The Chair of the CAB implemented a 5-step process for change management. Changes brought to the board are reviewed and approved by the CAB. Changes within the ES Process Computer Group (PCG), ES capital projects, other ES work, and Metro Transit (MT) construction change management occur outside the CAB. The CAB mainly reviews changes to systems that are managed by the IS department for the Council. The CAB maintains proposed changes in a spreadsheet. The CAB currently has around 50 members, although there is no formal process for becoming a member of the CAB. At present, not all members of the CAB attend meetings, and there is no record of attendance.

Within MT, the Transit Technology Advisory Committee and the Transit Technology Steering Committee perform some review and approval functions that affect technology change management. However, there are no clear roles or responsibilities for those groups related to the change advisory function. IS does manage the majority of identified technology changes for MT. Not all technology changes on the infrastructure side of MT are required to go through the CAB for review and approval. MT uses service level agreements with the IS department to manage some technology changes. The MT units mediate upgrades and changes via other division level processes and procedures for change orders.

ES doesn't have a central, documented technology change management procedure or separate CAB. The ES PCG group handles SCADA system changes. According to the Tech Coordination Manager, ES has practices it uses for change management related to specific technology projects. ES PCG group practices are not formally documented and do not specifically link to best practices. Furthermore, ES PCG group practices have not been periodically updated.

Objective

This audit evaluated the activities the Council has developed and implemented for change management, including controls implemented by the CAB and Ivanti Service Desk ticketing system. This audit evaluated change management policies, procedures, work instructions, job aids, and any tools used to manage technology changes and the extent to which practices minimize business and technology security risks. The audit reviewed the Council's adherence to NIST guidance regarding change management. Audit considered the Council's *Thrive MSP 2040* outcomes of Stewardship.

Scope

The scope for this audit considered change management activities for information systems hardware and software from 2021-2022. The audit examined all available change management documents, policies, procedures, work instructions, and job aids, as well as tools used in change management

---

[3] CIS Critical Security Controls, Version 8. https://www.cisecurity.org/controls/v8.

activities, including those activities affecting CAB processes and Ivanti Service Desk ticketing processes.

Methodology

Audit conducted interviews with various managers and staff in the IS department, and ES and MT divisions to review the processes behind change management. Audit reviewed existing documents for adherence to change management best practices from NIST and CIS.

Limitations

Audit noted significant barriers to analyzing user administration activities due to a lack of activity documentation in the form of policies, procedures, work instructions, or job aids. Technology Changes tracked on technology change tickets are not documented, which limited Audit's ability to review change management controls in use.

Recognition

Program Evaluation and Audit appreciates the assistance from the IS department, and ES and MT divisions provided during the audit. We are encouraged by the response to the issues identified and the recommendations made within this report. Council staff were forthcoming and helpful during interviews.

Observations

The Council does not currently have technology change management policies, procedures, or standards informed by industry best practices.

The Council does not have documented policies, procedures, work instructions, or job aids regarding technology change management. Council Staff manage changes in an informal, undocumented manner and do not consistently apply technology change management standards across all Council divisions. The IS department, and the MT Bus Rapid Transit business unit, and ES division use change management checklists. ES staff also document some processes via “practices” documents. ES capital projects use process control narrative (PCN) documents to note processes and specifications when technology is deployed through construction projects. IS and ES also use software solutions to document and manage changes for the Council. MT staff currently allows the IS department to execute change management for most of Metro Transit’s technology changes.

The Council’s *Technology Governance Policy (TECH 1-2)* requires the Regional Administrator to work with the Enterprise Services Planning Team (ESPT), which consists of division level senior executives, to commission the development of effective technology procedures and standards. Per the Council’s *Technology Governance Policy (TECH 1-2),* the ESPT should gather input from individuals with extensive knowledge of change management and input from individuals affected by the technology standard.

Neither the Regional Administrator or the ESPT facilitated the development of a change management policy, procedure, or technology standards based on industry best practices for the Council. Without effective change management procedures or standards, controls may fail to manage risks leading to higher costs, greater downtime, and project delays. The Council could also be exposed to operational risk due to mismanaged changes causing unplanned service interruptions, budget overruns and missed milestones.

Recommendation:

1. The Regional Administrator should ensure that formal change management policies and procedures and the required technology standards are developed based on industry best practices for the Council’s divisions.

   Management Response: *Pending*

   Timetable: *Pending*

   Staff Responsible: *Pending*

   Audit Follow-Up: Confirmation

2. The Regional Administrator should ensure procedures for change management outline the responsibility of the CAB within the procedure and standards based on industry best practices. Senior management should hold the divisions of the Council accountable for ensuring support and adoption of technology change management standards.

   Management Response: *Pending*

Timetable: *Pending*

Staff Responsible: *Pending*

Audit Follow-Up: Confirmation

The CAB does not have formal authority, defined roles, or responsibilities for technology change management activities.

The CAB does not have the authority to review and manage all technology changes for the Council and its divisions. The Council manages some, but not all, technology changes through the CAB. The CAB does not have an established charter or sponsor to assist it and provide oversight as it facilitates its duties. Currently, the CAB does not issue documented, formal approvals. Monitoring, reviewing, and oversight activities associated with technology change management are done on an ad-hoc basis and are not standard across the Council.

The Regional Administrator and the ESPT did not grant the CAB authority for technology change management. The ESPT did not establish a sponsor for the current CAB structure to create oversight and accountability. Additionally, the Regional Administrator did not commission or approve procedures and standards based on industry best practices to guide the activities of the CAB.

Without delegated authority for roles and responsibilities, the CAB cannot ensure it meets its desired business and security objectives related to technology change management. Without the CAB to review and approve changes, the Council is exposed to operational risk, possible system failure, or increased technology project costs. With IS, MT, and ES sometimes leading separate change management processes without effective standards, there is inconsistent management of technology changes for the Council. Without proper oversight of system changes, the Council could experience system functionality issues, increased downtime, or project delays.

Recommendation:

1. The Regional Administrator should formally charter and ensure the appropriate Sponsor(s) are established to ensure the CAB has the authority to oversee and recommend approval or rejections for changes for the Council.

Management Response: *Pending*

Timetable: *Pending*

Staff Responsible: *Pending*

Audit Follow-Up: Confirmation

2. The Regional Administrator should ensure the CAB uses technology standards and industry best practices for change management, as mandated by the *Technology Governance Policy (TECH 1-2)* and Council Policy and Procedure Framework.

Management Response: *Pending*

Timetable: *Pending*

Staff Responsible: *Pending*

Audit Follow-Up: Confirmation

Conclusions

Technology change management, at its best, is meant to prepare, support, and enable individuals and organizations to execute changes to information products and systems. Technology changes at the Council are currently left to the different departments and divisions to execute with no formal and effective process to identify, document, and control changes within the Council. When senior management establishes policies and procedures that mandate the use of technology standards informed by industry leading practices, management promotes risk mitigation, and ensures technology adds value to the organization and staff in meeting their business objectives. When senior management supports the CAB with a written charter, management sponsorship can help mediate technology changes, change reviews and approvals. By empowering the CAB, the organization can further maximize value and mitigate change management risks.

February 3, 2023
Matthew J. LaTour, Director, Program Evaluation & Audit
Chief Audit Executive

Appendix A

Program Evaluation and Audit recommendations are categorized according to how Audit will follow-up on them. The categories are:

- **Retest —** Audit will retest the area using the same or similar procedures after a recommendation has been implemented and sufficient time has passed for the changes to take effect. The retest will take place on a specified timetable. The recommendation will be closed once the change has occurred. A new audit project will be opened for retesting and any new findings will include new recommendations.
- **Confirmation —** Audit will confirm that an adequate risk response has been completed on the agreed upon timeline. The recommendation will be closed once the change has taken place.
- **Assess Risk —** Audit will not plan for specific follow up to these recommendations. Audit will discuss the area as part of its annual risk assessment activities and consider future audit work in the area.

Distribution List

All audit reports are reported to the general public and are available on *www.metrocouncil.org*. This audit report was distributed to the following parties:

- Members of the Audit Committee
- Regional Administrator
- General Manager/Division Director
- Department Director
- Process Manager

390 Robert Street North
Saint Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org