INFORMATION TECHNOLOGY AND ASSET MANAGEMENT AUDIT

Program Evaluation and Audit

***PER MINN. STAT. § 13.392, SUBD. 1**: DATA, NOTES AND PRELIMINARY DRAFTS OF REPORTS CREATED, COLLECTED AND MAINTAINED BY THE METROPOLITAN COUNCIL'S PROGRAM EVALUATION AND AUDIT DIVISION ARE CONFIDENTIAL UNTIL THE FINAL REPORT IS RELEASED OR ACTIVITY ON THE PROJECT IS DISCONTINUED. PLEASE DO NOT CIRCULATE THIS DRAFT TO ANYONE BEYOND THOSE DIRECTLY INVOLVED IN DEVELOPING THE MANAGEMENT RESPONSE.*

June 22, 2021

METROPOLITAN COUNCIL

Background

According to the Information Systems Audit and Control Association (ISACA); a primary element of an effective risk management process is to identify and collect relevant data on technology assets to identify threats, vulnerabilities, and classify risks. In 2018, the Metropolitan Council's division leadership adopted a Technology Governance Framework based on ISACA's COBIT 5 framework for the governance and management of IT, which provides a basic overview of technology asset management industry practices. Additionally, starting in Federal fiscal year 2020, the Council is required by the Federal Transit Administration (FTA) to "establish a process to develop, maintain, and execute a written plan for identifying and reducing cybersecurity risks that includes testing and use of approaches, standards, and best practices developed by the National Institute of Standards and Technology (NIST)." Typical assets associated with information and technology include information and data, hardware, software, documents, and personnel. Additionally, inventories of technology should account for asset value, criticality, and sensitivity to properly identify risks and appropriate controls. The likelihood of occurrence and impact of a threat exploiting a vulnerability is central to protecting and managing technology assets. Leading practices in hardware and software asset management, as noted in the NIST Framework for Improving Critical Infrastructure Cybersecurity, include integrating the technology asset management system with the organization's help desk function, technology configuration management, change management, and patch management.

The work of the Council is spread across five divisions with various mission and business objectives, which has led to elements of information and technology asset management being decentralized. Through Program Evaluation and Audit risk assessments, consultations, and audits from 2015 to present, it has been observed that the degree of centralization is additionally complicated by the number of asset owners. For some network infrastructure, Information Services (IS), Metro Transit, and Environmental Service may have different roles and responsibilities depending upon asset type and asset location driven by division level decisions. A decentralized information and technology asset inventory can lead to increased risk that technicians are unable to execute effective controls in inventory and configuration management. Reviews of existing controls and residual risk are necessary to ensure that asset inventories of data and technology assets support the continuity of operations and meet required business objectives. Recent initiatives through Audit's Technology Governance consultation have promoted the creation of procedures and standards regarding technology inventories, technology service management, change management, and patch management, but periodic audits have not been conducted to determine the current technology state of technology inventories, service management, and configuration management practices. The Technology Governance consultation additionally highlighted the fact that the Council does not have asset management software for technology that provides fully integrated functional needs.

Objectives

The objectives of this audit were to:

Confirm and document inventory practices and configuration management at time of deployment for Council hardware and software.

Measure the maturity of the Council's technology asset management program across and within the five divisions against leading practices in technology asset management.

This audit considered the Council's Thrive MSP 2040 outcomes of Sustainability, through measuring if practices preserve technology capacity and productivity, and Stewardship through determining the extent to which practices support orderly and economical asset management. Additionally, the audit will

consider the Thrive 2040 Principles of Integration by measuring cross-divisional synergies and Accountability by confirming the level of monitoring and evaluation of processes and practices in Technology Asset Management.

Scope

Technology hardware and software asset management from May 1, 2019 through December 30, 2020 from across the Council's five divisions were reviewed for this audit. Though the initial scope was intended to end in April 2020, the realities of the COVID 19 Pandemic extended audit work into December 2020. Technology Governance practices were not reviewed for Technology Asset Management and will be reviewed within the Technology Governance Audit in 2021. Given the Heywood and Robert Street building refresh cycles, some processes that span 2018 and 2019 are in scope, as the refresh cycle is a multiyear effort. Additional reviews of technology procurement and deployment during the COVID 19 Pandemic are also in scope. This review includes technology asset categories including: Local Area Network (LAN), Wide Area Network (WAN), Desktops, Servers, Printers, Mobile Devices, Network Appliances, Network Sensors, wireless, and any other special asset categories designated by the Council. As the Technology Governance framework is currently being implemented, Change Management and Patch Management will be scoped out of this review for inclusion in future audit plans, as Council Standards are developed. Configuration management is in scope to ensure that at the time technology assets are deployed, technology configurations are confirmed and documented.

Methodology

TAM policies and procedures were reviewed across all five divisions to understand the maturity of technology asset management that exists at the Council, as well as variation in management practices within each division. Interviews were also conducted with several Council staff to gain an understanding of their asset management processes, roles and responsibilities, and what steps are taken when constructing asset management policies, procedures, work instructions and/or job aids. The information obtained from reviews and interviews was then compared to industry leading practices from the National Institute of Standards (NIST) for hardware and software asset lifecycle management and planning, software licensure management, and configuration management at asset deployment.

OBSERVATIONS

Technology Asset Management procedures and job aids lack comprehensive coverage of all IT and OT asset management areas, lack clear definition of roles and responsibilities, and are not periodically reviewed.

Technology policies, procedures, work instructions, and job aids affecting Technology Asset Management have not been periodically updated or reviewed. In observing the policy or procedure last review date, half of the technology of policies or procedures that directly or indirectly affect technology asset management were reviewed within the last 5 years; the other half have not been reviewed within the last 5 years, four of which were last reviewed over 20 years ago (see Appendix). Recently, the Metropolitan Council established a Policies and Procedures Committee, and has acquired a system, Policy Central, to assist with logging, reviewing, and approving Council policies and procedures. The Policies and Procedures Committee has begun to set timelines for review cycles, but implementation is not complete. At present, practices around policy and procedure review are being established. Further, future review timelines only apply to policies and procedures housed in the new policy and procedure framework, and therefore for now exclude both Job Aids and Work Instructions. Additionally, current policies and procedures do not clearly document roles and responsibilities to indicating who is responsible for the maintenance and implementation of policies and procedures.

Policies and procedures for a number of key Technology Asset Management either do not exist or are out of date for related Information Services functions. These include documentation of processes as specific as the LANDesk Ivanti service ticket creation process for asset deployment and disposal, or as broad as Technology Asset Management planning, Equipment Receiving, Equipment Disposal, Device Refresh planning, Configuration management at time of deployment for various devices, Lifecycle Management planning, and Acceptable Use. Additionally, Technology Asset Management metrics are not documented in any procedures or guides. For instance:

- No defined procedures exist for how to classify IT Service Management tickets in the Ivanti system for technology asset deployment or disposal: it is left to the Service Desk staff to determine what ticket type should be used and what ticket type or status should be applied to IT asset management service tickets.
- The Service Desk does not appear to have a method of recording if an old asset was recovered in cases when new technology assets are ordered. Recording of old asset IDs and asset recovery was not consistent for tickets for damaged assets, end of life asset replacements, as well as asset replacements for issues encountered while working from home.

The Council has not established a materiality threshold and tracked assets of material value that were brought home or purchased for working remotely during the COVID pandemic. Specifically, technology assets were not consistently checked-out by employees who took Council equipment to work from home. Submitted tickets included records that were incomplete: some tickets were left blank, while many did not include asset ID or other important information. IS did track assets that were purchased and distributed by the department to work from home in two ways; one list was maintained in a SharePoint tool used by IS to log requests from division Operations Chiefs for technology, and another entry was made in LANDesk when assets were received by the council. At present there is no process in place to verify assets with a material value that were taken home or distributed to work from home will be returned to the Council when employees begin to return to the office, or how technology assets will be managed if working remotely is extended or greatly expanded in the future. Without verifying technology assets that were taken from Council worksites or assets distributed by IS to work remotely, it is difficult to attest to the integrity of the current technology asset inventory.

Per NIST guidelines, policies and procedures should address all NIST control families. NIST best practice guidance also recommends that policies and procedures for technology asset management should: be updated on an established periodic basis; include defined roles and responsibilities indicating who is accountable, responsible, informed and consulted regarding reviewing and updating technology asset management policies and procedures.

Without formally documented procedures for technology asset management and an established materiality threshold for assets, the Service Desk may not be able to optimize service levels for technology asset management and adequately log services provided via standard asset management metrics. Without standard procedures, work instructions, or guides, Technology Asset inventories may not be periodically conducted, and technology assets deemed materially important could go missing or be lost, replaced before the end of the asset's useful life, or conversely assets may be left active after the end of their useful life. Without documented procedures, work instructions, or guides, staff turn-over could result in the loss of substantial institutional knowledge, and cause inconsistency and discontinuity in technology asset management.

Without formally defined review cycles, policies, procedures, and controls for technology asset management may not be reviewed to confirm processes incorporate best practice security principals. Without formally defined roles and responsibilities, divisions or departments may implement asset management procedures or work instructions inconsistently and control objectives may not be met.

Recommendation(s):

1. The Council and its divisions should develop formal information services management work instructions or job aids to standardize the use of service ticket types for technology asset management that clearly define and document when each ticket type is to be used and what information should be documented by ticket type.

   Management Response:

   Staff Responsible:

   Timetable:

2. The Council and Council divisions should formally define and document roles and responsibilities for all technology asset management policies, procedures, work instructions, and job aids. Documentation of roles should denote who is responsible, accountable, consulted, and informed for specific technology asset management activities, decisions, and deliverables. IS and Division staff should define and document a formal review structure that states how often policies, procedures, work instructions, and job aids should be reviewed and describe the process for their review. A materiality threshold should be specified to confirm that technology assets above a specified threshold are subject to policies, procedures, work instructions, or job aids that are developed. Policies, procedures, work instructions, or job aids should consider addressing future remote work in the event that working remotely is extended or more widely used in the future.

   Management Response: ____ and ES will work to document roles and responsibilities for asset management as well as a materiality threshold to designate when a process must adhere to policies, procedures, work instructions, or job aids.

   Staff Responsible: ____ and Roger Knuteson, ES

Timetable:

3. The IS Department should develop a procedure to ensure that when Council employees return to work onsite, hardware loaner equipment distributed by IS during the pandemic and technology assets taken home by employees to work remotely are returned to the Council with a given materiality threshold. The procedure should additionally confirm controls for Employees who will continue to work remotely, and how deployed assets will be tracked and managed while working remotely.

   Management Response:

   Staff Responsible:

   Timetable:

Technology Asset Management relies on multiple inventory information systems, and there is not a standard set of asset management attributes tracked by within systems.

Assets are tracked in seven different tracking databases or systems across the council. The three main systems are:

- LANDesk (regularly called the Ivanti system, it is used largely by the IS department),
- Process Computer Group (PCG) Parts database is an in-house solution created and used by the ES PCG team, and
- TXbase, which is used to integrate maintenance, inventory management, purchasing and finance for Metro Transit business processes, and as such it is not a traditional inventory system.

Inventory tracking systems across the council track a variety of inventory attributes. Differences in quality and completeness of attribute tracking exist between the inventory systems used for technology asset inventories across the Council. Variations include the number of attributes fields available, and the kinds of attributes tracked, as well as how frequently data was logged in the attribute field. For Technology Assets, there are approximately five core attributes, along with three other recommended attributes that should generally be tracked that link to key controls recommended in guidance provided in the NIST Framework for Improving Critical Infrastructure Cybersecurity. At a minimum, the key core attributes consist of asset name and number, asset type, location, and asset owners (indicated by department, and division). These are considered core attributes. The organizational importance of an asset should also be tracked, based on: Cost (replacement cost if an asset were lost); criticality of the asset (impact of loss of an asset); and sensitivity (does the asset include low, medium, or high-risk data). For assets inventoried in the Ivanti system, 33% of tracked assets (2,310 of 6,860) track all core attributes. For assets tracked by ES, 44 of the 96 most recently logged assets (45%) track all core attributes.

	Core attributes tracked	Location attribute contains data
IS (Ivanti)	33%	100%
ES (PCG Database) *	45%	45%

Table 1

*Note that the assets observed in the PCG database are the 96 most recently entered items, not the entire database.

For both IS and ES assets, the location attribute is a non-standard field, and there is variation in the format of data entered. Data logging practices recently changed to include tracking the location of ES assets, and the observation of 45% of assets that do include location reflect the more recent asset data entry practices. Some location entries are sufficient to locate the asset (i.e., locations specify a closet or a cubical like "FTS/2/Network Closet" or "390/1/Cube07"). Other location data entries are too vague or non-specific, and only state an asset is at a specific train station or a data center, without situating the asset's location at said station or data center (i.e., locations specify things like "Platform/Westgate" or "BLEPS/1/Network"). Analysis suggests at least 600 of the roughly 3000 ETS-owned devices have insufficiently clear locations in the Ivanti system; for a further 2000 assets, the location apply naming conventions for which no procedure or guide has been developed specifying how to interpret the location entry. It is also uncertain how accurate location data is; for instance, 799 assets are listed as being in a "parts room", but there are no specified regions within the parts room, and no periodic physical audits are conducted to confirm the integrity of this attribute data.

All three main systems record an asset's "type". The classification used for asset types varies in levels of specificity. At certain times, asset type links to assets like laptops, tablets, or network switches, which are what the IT Service management (ITSM) best practices would classify an asset class. In other instances, asset type is used by Council divisions to denote things like desktops, network appliances, or servers, which ITSM best practices would generally designate as an asset category. Asset category and class designations help to specify asset classification within the inventory to maximize IT asset inventory best practices, given that asset classes like laptops, desktops, and network switches can be used across multiple IT and OT environments, including network segments and/or data centers.

Among the seven tracking systems, there are at least four different departments across the Council tracking assets. IS tracks all technology assets in the LANDesk Ivanti system, including assets serviced by IS Infrastructure, Network and Telecom, Desktop and Service Desk departments, including many IT assets owned by Metro Transit. The ES PCG group tracks some IT and all OT assets for ES in an in-house database; the PCG Parts system tracks assets like those tracked in Ivanti, including servers, laptops, desktops, monitors, network switches, and printers. Metro Transit has a technology Project Manager who is working to compile information on the ten departments that independently maintain IT/OT inventories. MTS has an Onboard Technology Manager who facilitates contracted services and works with a Business Systems Analyst to track mobile gateways, mobile data terminals, camera systems, bus mobile validators and fareboxes, as well as RFID devices. Within Metro Transit, a variety of asset types are tracked in manual tracking systems. Three asset types are manually tracked using only the "asset tag" attribute, and thirteen assets are tracked in manual and mutable tools, including Excel sheets, Visio documents, or a less formal database.

Technology Asset inventories were not observed for MT and MTS managed assets, due to restrictions related to the pandemic. Additionally, due to the large number of tracking systems used and the distributed nature of attribute tracking, Audit was unable to review attribute level data. Per division staff, only two asset types tracked by Metro Transit track all core attributes. Tracking of core attributes by MTS is unclear; core attributes appear to be tracked between the Ivanti and TXbase systems, though all core attribute information may not be compiled in one system.

	# of tracking systems	# of asset types tracked
MTS	5*	72
MTS	3	5

Table 2
*Including various manual systems such as: spreadsheets, Visio documents, and other manual tracking systems of asset tags

Across all Council divisions, there is no documentation that inventory controls have been mapped to an information security control framework. There are no policies or procedures mandating the existence or use of a council-wide control framework. Council Technicians may employ some best practices for IT and OT asset management, but no department or division has formally documented technology asset management practices via policies, procedures, job aids, or work instructions. A lack of mapping current IT and OT asset management controls and not mapping them to information security control framework creates the risk of controls do not adequately track core attribute data and limits the integrity attribute data. Not tracking all core and recommended attributes may mean inventory data are not sufficiently useful to inform decision-making or planning. Tracking that does not include periodic inventory audits may make reports on those assets unreliable, negatively impacting planning and IT service management.

Recommendation(s):

1. The Council and its division should track assets in a centralized system of record. Tracking should at a minimum track all core attributes, as well as additional attributes to serve business objectives and mitigate information security risks. Asset management tracking process should be well documented. In cases where a non-standard or non-centralized system of record is used, policies or procedures should designate an exception processes, detailing when an exception can be granted, and what baseline attributes should be documented in noncentralized systems.

   Management Response: *____ and ES will work to determine needs technology asset inventory needs, track assets in a centralized system of record, and document cases where technology assets must be tracked centrally or may be tracked in non-centralized systems of record.*

   Staff Responsible: *____ and Roger Knuteson, Manager, Process Computer Group*

   Timetable:

Technology Asset Lifecycle Management practices are not formally documented for all assets

Technology Asset lifecycle planning and management practices exists, though practices vary across the Council and its divisions. Lifecycle management practices range from having informal refresh planning documents to relying on budget planning processes and institutional knowledge to meet lifecycle planning functions. For some assets, divisions do have formal lifecycle management plans, but planning has only been implemented in the last few years and as yet does not constitute a complete cradle to grave technology asset management plan.

The NIST Framework for Critical Infrastructure Cybersecurity provides lifecycle planning requirements and guidance including standards which recommend determining a mean time to failure (MTTF) for certain assets and that substitute components/assets should be on hand to replace these assets before they fail. Guidance also speaks to developing metrics that assist in estimating the date assets will fail to assist with planning for asset replacement.

Not having a formal asset lifecycle management opens the Council to unnecessary physical and information security risks, particularly with older assets. Additionally, there are also potential financial risks in that there may be unanticipated costs with unexpected failures. Additional costs can be incurred in performing maintenance on older assets whose parts may be difficult to acquire and keep in stock. Due to the lack of formal policies and procedures for Technology lifecycle planning, the Council may not be able to perform cost-effective strategic asset management planning.

Recommendation (Essential)

1. The Council should develop a set of centralized, formally documented Technology Lifecycle Management Plans for IT and OT Assets, or Council divisions should develop division specific requirements for technology asset management planning. In either case, the IT and OT asset lifecycle management plans should be informed by a comprehensive information security control framework, with plans established on information security principles.

   Management Response: ____ and ES will work to determine business needs for Technology Asset Life Cycle planning and document practices for all assets above a to be determined materiality threshold.

   Staff Responsible: ____ and Roger Knuteson, Manager, Process Computer Group

   Timetable:

Configuration Management for technology asset baseline confirmations are not based on formal procedures, consistently documented, tested, or audited.

Configuration checklists or baseline configuration settings are established for some technology assets managed by Council divisions. However, there are multiple approaches to managing baseline configurations across the Council. Baseline configurations that do exist are based on IT and OT technician's professional expertise, and configurations do not always follow established, documented configuration checklists. For these configurations, technicians have not documented reviews or audits of current configurations implemented to confirm settings are based on industry leading information security principals. In a few instances, asset configurations are being tested after they have been configured, but no procedures or processes are in place to document roles and responsibilities and confirm separation of duties for initial configurations and configuration testing. Additionally, there are no configuration audits being periodically performed to confirm baseline configuration settings at the time an asset is deployed are based or informed by NIST CI information security principals.

The NIST Cybersecurity Framework for Critical Infrastructure provides guidance on how to establish baseline configurations and document configuration in a checklist format. Not having configuration management plans and checklists based on information security principals could lead to assets not being configured to mitigate for vulnerabilities, which leaves Council assets vulnerable to known threats.

Recommendation (Essential):

1. The IS department and Council divisions should develop standard Configuration Management processes that are documented, with methods based on an established information security control framework to ensure asset configurations are maximized, documented in formal IT and OT configuration management plans. Baseline configurations and checklists should additionally

be periodically audited to confirm controls are implemented appropriately to protect council assets.

Management Response: ____ and ES will develop baseline configurations and develop standard configuration management plans and document practices for all material technology assets.

Staff Responsible: ____ and Roger Knuteson, Manager, Process Computer Group

Timetable:

Asset Disposal

The Council uses two vendors for the disposal of IT and OT assets. Both vendors currently possess a National Association for Information Destruction (NAID) certificate, but the Council had been using one for approximately four years before they obtained their certification. There has been some initial level of review of both vendors and there are future plans to follow up on vendors with monitoring and auditing activity. Currently, there is no documented procedures related to IT/OT asset disposal vendor management. Per NIST guidance, organizations need to determine what media needs to be sanitized, how the assets will be tracked/documented through disposal, verification activities, and secure the assets during the disposal process.

While a NAID certification is not a requirement, certification requirements ensure that best practices for IT and OT asset disposal and sanitization meets Payment Card Industry Data Security Standards (PCI-DSS) and Health Insurance Portability and Accountability Act (HIPAA) requirements. Without the NAID certification and vendor monitoring or auditing, the Metropolitan Council cannot be assured that IT and OT asset disposal vendors are properly sanitizing Council assets, which could lead to the loss of sensitive or confidential data, misuse of secure data, litigation, and/or reputation risk for the Council.

Recommendation (Essential)

1. Council divisions should standardize the criteria to confirm the IT and OT Asset disposal vendors securely destroy assets based on specific federal, state, and/or industry specific requirements. Council divisions should also develop and formally document their process for performing regular monitoring/auditing activities.

   Management Response: ____ and ES will develop and document technology asset management disposal processes to ensure secure asset destruction.

   Staff Responsible: ____ and Roger Knuteson, Manager, Process Computer Group

   Timetable:

Software Licensure is not consistently tracked in an asset management system, and license tracking processes are undocumented.

There is no centralized system in place to track software licenses across the Council and its divisions. The IS Infrastructure team has stated that they use an automated tool to monitor the licenses in use for Microsoft products. For all licenses other than Microsoft Office 365, information about what software licenses in use is gathered manually, if at all. License tracking process owners lack documented processes related to software licensure management. Additionally, no audits have been performed on

software license tracking and no documentation of current auditing or monitoring practices was available.

Per NIST Standards and ISACA guidance, organizations should create inventories of software license information containing license type, software version numbers, number of licenses purchased, number of licenses in use, computers where software in installed, and date purchased, and track the use of licensed software, ideally via an automated system. Without automated or manual tracking processes, the Council could use more software licenses than it has purchased, or could run out of licenses, putting the Council at risk of substantial fines or unplanned added costs. Licenses may not be purchased in the most cost-effective manner, or the Council could incur unnecessary costs by purchasing more licenses than are necessary. There is no Council policy or procedure that mandates the tracking of software licenses or that any monitoring activities need to be performed. For many software licenses, management and tracking of licenses is handled by the division or a department within a division and not in a central software asset management system. Technology asset management inventory software has not been maximized to track software or software licenses, or to allow for the tracking of recommended software license attributes.

Recommendations:

1. Documented procedures, work instructions, or job aids should be created to mandate the tracking of software licenses, materiality thresholds regarding what software licenses require tracking, and what software attributes are to be logged and tracked. The Council and its divisions should consolidate software licensure efforts (procurement, distribution, cancellation, etc.), and consider the use of a centralized software licensing management system. The Council Divisions and the IS department should consider using an automated scanning tools to monitor software licenses when possible, as well as developing and documenting a method to monitor software licenses purchased by the Council and Council Divisions.

   Management Response: ____ and ES will work to document software license tracking processes above a given materiality threshold in work instructions or job aids and consider the use of a centralized automated system for license management.

   Staff Responsible: ____ and Roger Knuteson, Manager, Process Computer Group

   Timetable:

IS Sole Source List

The IS Department has worked with Council divisions and departments to acquire hardware and software assets that require ongoing maintenance, hosted service, and third-party support via the IS Sole Source List. The IS Sole Source List is functionally used as a list of hardware and software vendors for which previous procurements have already been completed. Items on the “sole source” list are added to the list to seek approval for ongoing maintenance and support service costs that result from continued use of the hardware and software assets. The Council’s Procurement Procedure addresses Sole Source procurements and provides the guidance that “Sole source procurement of Original Equipment Manufacturer (OEM) repairs, parts, equipment and systems, software maintenance and support, or other services that are require on a continuous basis may be authorized on an ongoing basis.” The procedure additionally states that “Sole Source Procurement must be used with care on an exception basis only and must be justified for each occurrence.” The Sole Source process does not specifically detail any requirements for the IS Sole Source List, separate from other sole source procurements.

The IS sole source list is reviewed and updated on a periodic basis. Each item on this IS sole source list has a business owner who determines and vets the justification for that specific item before the list is reviewed and approved by Information Services, Finance and Budget, Procurement, and eventually the Council. Some items on the IS sole source list are stated to be only provided via IS sole source vendors, though in practice some vendors appear to be added to the list for a variety of reasons, including:

- There is a significant cost associated with switching to another vendor providing comparable services, hardware, or software
- For software license renewals and software upgrades available only from a developer/supplier for an existing license agreement
- IT supplies from a previous supplier required to ensure consistency of required IT supplies

There is minimal amount of required information about how the basis for the price of items on the IS Sole Source List is reached, and how the Council can be assured of the reasonableness of the price for items on the IS sole source list. At the beginning of this audit the process and justification for adding, keeping, or removing an item on the IS Sole Source list was not clearly documented in policy or procedure. It was also not clear how or if the procurement Sole Source form was used in conjunction with the IS sole source list. In late 2020 the Procurement department created the Sole Source Review Team (SORT) and developed a new process to review both IS and non-IS sole source requests. The Procurement department was able to provide documentation on the new process, those involved in the Sole Source Review Team (SORT), as well as a spreadsheet noting reviews and decisions the SORT team has completed for the 2021 IS Sole Source list. While the new SORT process and team add clarity to the sole source process, there are still concerns with the methods of research employed. The only research that was documented was an internet search to determine if a vendor was a reseller or not, and if IS approved the vendor as an IS sole source vendor. There is also a concern on how cost reasonableness is justified with supporting documentation for the IS Sole Source list, because the SORT process does not provide details or guidance on documentation requirements. The Procurement department's SORT Team process has improved controls around the IS Sole Source list, however, the updated process is not included in standard Council procedure and has only been operable for less than a year.

While the provisions of the Federal Acquisition Regulations (FAR) are not required for Council acquisitions, they are considered "best practice" that should be employed when recipients of federal grants are acquiring assets. Specifically, some of the more pertinent FAR 6.303-2 requirements include a description of the product or service including estimated costs, justification containing sufficient facts and rationale, a description of the efforts made to ensure offers were solicited from as many sources as practicable, and a description of the market research conducted. If the procurement procedures for providing justification are not clearly defined and reviewed, and efforts to ensure vendor sourcing is practicable are not documented, the Council may continually approve a sole source item that may not actually need to follow the sole source process, which could lead to inefficiencies, unnecessary expenses, and/or the perception that the Council is favoring a particular IS vendor or contractor. In addition, there is a potential for added inefficiencies and lack of accountability that could occur when a defined signature authority process isn't used, as opposed to the more time-consuming IT Sole Source process.

Recommendation (Essential):

1. The Procurement SORT team should update processes to ensure the requirement to maintain clear, detailed, and documented justifications for why each item is on the IS Sole Source List. The IS Department's justification forms should be updated to include specific categories of

expenses that are eligible for an exception to the Procurement Procedure as an IS sole source item, and when Division and IS level approvals are required.

Management Responses: Procurement will work to update SORT Team procedures to ensure detailed justifications are supported and documentation is maintained.

Staff Responsible: Jody Jacoby, Director, Contracts and Procurement

Timetable: September 30, 2021

2. Procurement and IS should review the process to determine if some of the IT Sole Source items can be shifted to a signature authority process to increase efficiency and accountability.

Management Responses: Procurement will work with IS to evaluate if signature authority processes could add efficiency and accountability to procuring IS Sole Source Items through SORT team processes.

Staff Responsible: Jody Jacoby, Director, Contracts and Procurement

Timetable: September 30, 2021

Appendix

Policy Name	Years Since Review	Criticality/Risk Level
TECH 2-1 Information Security Policy	2	(Undefined)
TECH 2-1a Wireless Security Procedure	12	(Undefined)
TECH 2-1b Virus Protection Procedure	1	(Undefined)
TECH 2-1c Workstation Security Procedure	11	(Undefined)
TECH 2-1d Patch Management	11	(Undefined)
TECH 2-1e Password Procedure	10	(Undefined)
TECH 2-1f Reporting a Lost/Stolen Corporate Liable Asset	7	(Undefined)
TECH 2-1g Payment Card Industry Data Security Standard	5	(Undefined)
TECH 2-1h Inactive User and Vendor Account Management Procedure	1	(Undefined)
RF 7-2 Use of Council Property	22	(Undefined)
RF7-2a Expectations of Privacy in the Workplace	22	(Undefined)
TECH 1-1a Cell Phone Services and Equipment	8	(Undefined)
TECH 1-1b E-Mail and Intranet/Internet Usage	8	(Undefined)
TECH 1-1c Computer Usage	22	(Undefined)
HR 9-2 Security Policy	22	(Undefined)
HR 9-2a Identification Badges	2	(Undefined)
HR 7-3 Telework Policy	3	(Undefined)
HR 7-3a Telework Procedure	3	(Undefined)
TECH 3-2 Data Practices Policy	6	(Undefined)
TECH 3-2a Data Practices Procedure	5	(Undefined)
TECH 3-2b E-Discovery Software Procedure	1	(Undefined)
TECH 3-2c Records Management Procedure	12	(Undefined)
TECH 3-2d Cloud Services and Content Management Procedure	3	(Undefined)
TECH 3-2e Personnel File Data	4	(Undefined)
TECH 3-3 Document Management Policy	9	(Undefined)
Ticket creation procedure - Asset Deployment*	Policy doesn't exist	(Undefined)
Technology Asset Management Planning*	Policy doesn't exist	(Undefined)
Equipment Receiving Procedures*	Policy doesn't exist	(Undefined)
Equipment Disposal Procedures*	Policy doesn't exist	(Undefined)
Refresh Plan*	Policy doesn't exist	(Undefined)
Configuration checklists for various devices*	Policy doesn't exist	(Undefined)
Configuration management plan*	Policy doesn't exist	(Undefined)
Cradle to Grave / lifecycle management plan *	Policy doesn't exist	(Undefined)
Acceptable Use policy*	Policy doesn't exist	(Undefined)
Asset Management Metrics Guide*	Policy doesn't exist	(Undefined)

*Policies, procedures, work instructions, and job aids are recommended by NIST Best Practice Guidance, as are criticality levels.

390 Robert Street North
Saint Paul, MN 55101-1805

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