

# VENDOR FILE MANAGEMENT

*PROGRAM EVALUATION AND AUDIT*



**METROPOLITAN**  
C O U N C I L

## Contents

Highlights.....	3
Summary of Findings.....	4
Introduction.....	6
Background.....	6
Objective.....	7
Scope.....	7
Methodology.....	7
Limitations.....	8
Recognition.....	8
Conclusions.....	19
Appendix A.....	20
Appendix B.....	21

### What We Found

#### *What Needs Improvement*

The Metropolitan Council's process to create, update, and manage vendor files is inefficient due to duplicative processes and roles. Current process documentation is either inadequate or nonexistent, resulting in duplicate vendor files and vendor files that are still in the system after five years of inactivity. Additionally, vendor files are missing pieces of information such as Tax Identification Numbers (TINs), TIN types, addresses, and address descriptions.

We also found that staff are not evaluating conflicts of interest, and instead are relying on self-certification.

Finally, while reviewing the vendor creation and update process we found that private and confidential information was made available on Council internal systems.



### What We Recommend

The Metropolitan Council should:

- Have a better system in place to review for conflicts of interest.
- Train employees on conflicts of interest and data classifications.
- Remove duplicate vendor files, where applicable.
- Create or update procedures and documents related to vendor file management.
- Consolidate the vendor file creation and update process, if possible.

### Why We Did This Work

The purpose of this audit was to assess vendor file accuracy, identify duplicate entries, determine if file maintenance was performed, and identify if management is implementing best practices.

### What We Reviewed

We reviewed documents related to vendor file management, PeopleSoft data, audit logs, vendor file data on MetNet, industry best practices, and audits performed by other agencies.

### How We Did This Work

We interviewed Procurement, Finance, Risk and HRA staff to help understand the process, the systems involved, and the data that is in those systems. Audit also reviewed documentation related to vendor file management and performed desk reviews of requested data.

## Summary of Findings

Number	Description	Recommendation	Follow-up Action	Page
<b>Observation 1</b>	The process to create or update vendor files is duplicated across three departments.	Review the process to identify consolidation opportunities.	Confirmation	<a href="#">9</a>
<b>Observation 2</b>	Vendor account information change requests are not systematically verified.	Create and implement a procedure for verifying vendor changes and requests.	Confirmation	<a href="#">9</a>
<b>Observation 3</b>	5.3% of vendor files have not been used in 5 years.	Develop a central procedure for vendor maintenance.	Confirmation	<a href="#">10</a>
<b>Observation 4</b>	Vendor file contains duplicates, inconsistent naming conventions, and missing data.	Review existing documentation, identify duplicates, identify naming conventions. Create procedures.	Confirmation	<a href="#">11</a>
<b>Observation 5</b>	Procurement staff enter same vendor information up to 3 times per entry.	Meet with the BPSI integrator to identify vendor manager needs.	Confirmation	<a href="#">12</a>
<b>Observation 6</b>	Staff do not review the vendor file audit log.	Use the audit log and design a control in line with best practices.	Confirmation	<a href="#">13</a>
<b>Observation 7</b>	Staff do not review for conflicts of interest.	Identify fraud and COI indicators and test them. Create a policy to proactively identify COIs.	Confirmation	<a href="#">14</a>
		Create and implement COI training.	Confirmation	
<b>Observation 8</b>	Private and confidential data was made available internally.	Take measures to mask private and confidential information.	Confirmation	<a href="#">15</a>




		All staff involved in vendor creation should receive training on data classification.	Confirmation	
--	--	---	--------------	--

# Introduction

## Background

The Metropolitan Council maintains information on its vendors, suppliers, employees, and Housing and Redevelopment Authority (HRA) tenants and landlords, referred to as the vendor master file (**Table 1**). The terms “vendor” and “supplier” are used interchangeably throughout this report. Each file contains crucial information, including a vendor’s contact information, tax information, and other account information. The Metropolitan Council has thousands of suppliers, and it is imperative that the information in each vendor file is accurate. The file must be maintained to prevent confusion, mistakes, and to detect or prevent fraud.

**Table 1: Examples of Vendors**

Procurement	HRA	Risk
<ul style="list-style-type: none"> <li>Contractors</li> <li>Suppliers</li> <li>Governments</li> <li>Professional Organizations</li> </ul> 	<ul style="list-style-type: none"> <li>Landlords</li> <li>Tenants</li> <li>Housing Authorities</li> </ul> 	<ul style="list-style-type: none"> <li>Employees</li> <li>Insurance Companies</li> <li>Lawyers</li> <li>Claimants</li> <li>Hospitals</li> </ul> 

The Council has three departments that manage vendors, Risk Management, Procurement, and HRA. New vendors or changes to existing vendors are handled differently depending on the department that vendor interacts with. Finance staff also review submissions before the changes and additions are sent back to the Vendor Managers to update their individual systems.



For example, if it is a Procurement vendor, changes and additions are requested through the Vendor Request Form on MetNet. Any council employee can complete this form, which is then submitted to the Vendor Manager, who reviews the information and then creates the new vendor, updates information, or requests additional information. Afterwards, Finance staff review the transaction to ensure that the requested change was made.

All vendor information is maintained in the Council's financial system of record, PeopleSoft Financials. However, the Council's risk management claims system, purchasing systems, and housing systems all pull information from the system. Each system has its own administrator.

This audit was conducted in response to the 2022-03A Paper Check Processing Audit. As part of the Paper Check Audit, Program Evaluation and Audit staff received the vendor file for a routine fraud check. The vendor file had various, obvious maintenance errors and required additional review.

## Objective

This audit assessed vendor file management to ensure that information in the system of record is accurate, that there were no duplicate vendors, maintenance is performed, and best practices are implemented.

This audit considered the Council's Thrive MSP 2040 Outcomes and Principles of *Stewardship* and *Accountability*.<sup>1</sup> This audit furthers *Stewardship* by reviewing processes to ensure that the Council is efficient with its resources. The audit promotes *Accountability* by reviewing adherence to Council policies and procedures and maintaining accurate vendor files. Finally, it furthers the principles of *Integration* and *Collaboration* by encouraging staff to work together on evaluating existing practices and systems.

## Scope

This audit included all vendor files in the system of record at the Council and any policies, procedures, or other documentation related to vendor file management. It did not include reviewing payments to vendors or reviewing Information Technology General Controls for the systems housing vendor information.

## Methodology

Audit conducted remote interviews, researched best practices, and analyzed large data sets to determine if Procurement, Risk, HRA, and Finance were efficiently and effectively managing the vendor process and records. In order to assess the accuracy of information, Audit interviewed Finance, HRA, Procurement, and Risk Management staff to determine if they had processes and procedures for ensuring that data was accurate. This included how they verify change requests, if they had data entry standards, and what do the approvers do.

To determine if staff are maintaining vendor files, Audit interviewed staff from each area. Each department was interviewed to determine if they had documented maintenance standards or methods for maintaining the files. Additionally, Audit acquired and analyzed the vendor file along with the last payment dates. These active vendors were reviewed to see if they had been paid in the last 5 years.

---

<sup>1</sup> The Metropolitan Council. "Thrive MSP 2040."

A common finding in government vendor file audits is that staff had failed to disclose relationships with third-party vendors.<sup>2,3,4</sup> As such, Audit tested for potential conflicts of interest to promote *accountability, stewardship*, and ensure that the Council’s Conflict of Interest Procedure was implemented.<sup>5</sup> Audit acquired a list of active employees and their addresses, and then compared them to the master file. Any overlap in the supplier or HRA vendor files was flagged and passed to management for further review.

Information Technology General Controls (ITGCs) were not a part of this review. However, other agencies performed cursory reviews of access controls. Audit reviewed three months of the Vendor File Audit Log to determine if the appropriate personnel had made changes to the vendor file. For example, that HRA staff only modified HRA files. Audit interviewed Finance, Procurement, Risk, and HRA staff to determine “Appropriate Personnel”.

Audit reviewed the vendor files in PeopleSoft to determine if there were duplicate vendors and inaccurate data in the vendor files including missing data fields or issues with naming conventions.

Finally, Audit researched best practices for vendor file management by reviewing audits from other public agencies. Audit pulled the reports’ best practices and audit recommendations, then identified common themes.

### *Limitations*

Audit relied on Administrative Systems Support and Human Resources staff for PeopleSoft Financials and Human Resources queries. Additionally, Audit relied on managers to proactively review potential conflict of interests.

### *Recognition*

Audit would like to thank Procurement, Risk, HRA, Finance, Environmental Services, and Metro Transit staff for their cooperation and timeliness during this audit.

---

<sup>2</sup> Oseguera, J. and Bashaw, L. (December 2015). “Audit of the City’s Master Vendor File.” The City of Sacramento, California.

<sup>3</sup> Remias, L. and Hudome, G. (August 2019). “Audit of the City’s Vendor Master File.” The City of Virginia Beach, Virginia.

<sup>4</sup> BKD, LLP. (September 2018). “The Consolidated City of Indianapolis and Marion County Vendor Master File Assessment.”

<sup>5</sup> FM14-1C Conflicts of Interest Regarding Selections of Consultant and Vendors Procedure.



# Observations

## The process to create or update vendor files is duplicated across three departments.

The process to create or update a vendor file is duplicated in Procurement, HRA, and Risk Management (**Appendix B**). Each department has its own process variations that increases the process' complexity. These variations include Risk having their own form for changes to or adding new suppliers, and Procurement having to manually update vendor information in TXbase and WAM after PeopleSoft uploads data to either system. Staff referenced a decision to split the process between the three departments several years ago due to technology needs.

The Government Accountability Office's (GAO) Greenbook (pg. 56) states that "Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks." The risk to having duplicate processes unnecessarily increases the resources needed to create or update a vendor file and increases the likelihood of inconsistencies and potential fraud risks.

### Recommendation:

1. The processes should be reviewed to determine if there are ways to consolidate the process to improve efficiency, effectiveness, and consistency and then implement those methods.

### Management Response:

Management acknowledges there are currently three different areas of the business that is entering in vendor information. It is incredibly important to ensure timely payments to all vendors that vendor information is entered when received.

HRA and Risk work with their vendors to help get the information needed for payments. Procurement handles all other vendor set ups. It was divided to provide better customer service to all vendors.

It is also divided between the three areas due to different systems in Risk (Origami) and HRA (Happy) and Procurement (Txbase and WAM).

Management will document the vendor set up process in a policy and procedure so this process can be reviewed, and audited for consistency, effectiveness and efficiency in vendor set up areas. This document will also help analyze opportunities for a centralized systematic way of processing vendor set-up and changes.

**Timetable:** Documentation of a new Policy and Procedure completed by January 2023

### Staff Responsible:

Marie Henderson, Deputy CFO and Jody Jacoby, Director of Contracts and Procurement will co-lead this effort. Staff responsible for the new policy and procedure will be assigned Procurement staff; Tammy Prigge, HRA; and Amanda Martens, Risk

**Audit Follow-Up:** Confirmation

## Vendor account information change requests are not systematically verified.

Requests to change a vendor's information are undocumented and are not systematically verified. If the department verifies, each does it differently. Some departments require changes to be mailed in, others verify vendor information through Google or a call back. Best practices recommend having a "stringent, repeatable process for collecting, validating, and storing vendor information."<sup>6</sup> It could include methods such as call backs, standardized forms, or other forms of verification. This issue was caused by not having a centralized vendor management process at the Council. As such, no one was responsible for developing common verification standards. By not having a standard verification process, each department verifies differently, and the verifications are generally undocumented. This increases the Council's risk of vendor fraud or a fraudulent third-party gaining access to a vendor's information and changing it to their own.

2. Finance should create and implement a procedure for verifying vendor changes. Staff should identify a method for documenting change requests.

### Management Response:

Management acknowledges that a policy and procedure Council wide should be established, documented, and followed. This would include details of vendor set up and vendor verification, including checklist and any other data that would be retained for audit purposes.

Management is also implementing a banking number verification system to use the banking system to ensure the bank accounts are tied to the vendor.

**Timetable:** Banking system verification in place by September 2022. Documentation of a new Policy and Procedure completed by January 2023.

**Staff Responsible:** Marie Henderson, Deputy CFO and Jody Jacoby, Director of Contracts and Procurement will co-lead this effort. Staff responsible for the new policy and procedure will be assigned Procurement Staff; Tammy Prigge, HRA; and Amanda Martens, Risk.

**Audit Follow-Up:** Confirmation

## 5.3% of vendor files that have not been used in over five years.

Of the 17,110 vendors there are 914 vendors (approx. 5.3%) that have not been active in over five years. 752 are from HRA, 154 are from Procurement, and the remaining eight are classified as "Employee". Best practices indicate that vendor files should be reviewed on a regular basis and removed after 12 to 18 months of inactivity.<sup>7,8</sup>

Procurement staff recently (Q4 of 2021) began reviewing vendor files and removing those that did not have any activity in the past five years.<sup>9</sup> Meanwhile, the Risk department had recently reviewed their vendor files and removed those that did not have any activity in the past year. They did not coordinate with the other vendor managers. Finally, the HRA has not reviewed their vendor files in approximately

---

<sup>6</sup> Anastasakis, A. (March 2021). "Safety First: How to Handle Supplier Banking Data." *CPA Practice Advisor*.

<sup>7</sup> Strategic Audit Solutions, "Vendor Master Best Practices: Keeping It Clean Mitigates Risk", pg. 3.

<sup>8</sup> AvidXchange. (July 2017). "Master Vendor Cleanup: Best Practices for Year-End Closing", pg. 2.

<sup>9</sup> According to Procurement staff, five years is the maximum Council contract length.

three years. Previously, HRA staff removed files that did not have any activity in the past year, but the responsible staff member left the Council.

Having 914 vendor files that have not been used in over five years can be attributed to the fact that a procedure on when to review vendor files and when to deactivate them does not exist. Failing to perform regular vendor file maintenance increases the number of fraud opportunities and the chance that someone could use the wrong vendor file, which could result in the vendor receiving incorrect payments, payments to the wrong location, payments to the wrong vendor, or not receiving a payment at all.

**Recommendation:**

3. A centralized and controlled procedure should be developed that outlines when vendor maintenance should be done and when to remove inactive vendors.

**Management Response:**

Management acknowledges that standard practices for archiving inactive vendors should be documented and followed Council wide, for all systems used for vendor information.

**Timetable:** Documentation of a new Policy and Procedure to be completed by January 2023

**Staff Responsible:** Marie Henderson, Deputy CFO and Jody Jacoby, Director of Contracts and Procurement will co-lead this effort. Staff responsible for the new policy and procedure will be assigned Procurement staff; Tammy Prigge, HRA; and Amanda Martens, Risk

**Audit Follow-Up:** Confirmation

**Vendor files contain duplicates, naming conventions are inconsistent, and data is missing.**

Vendor file data has several quality issues and there are numerous duplicate vendors (**Table 2**).<sup>10</sup> Data quality issues include inconsistent naming conventions, TINs containing a string of 9s, and required fields that are missing information. Best practices indicate that organizations should avoid having duplicate suppliers to prevent fraud and sending duplicate payments.<sup>11</sup> One of those best practices also is to establish and maintain a clean and accurate vendor master file.

PeopleSoft can check for duplicate TINs, but it is unclear how effectively or consistently this function is used. Additionally, the Supplier Entry and Update document implies that staff can create duplicate vendors under certain conditions due to system limitations and user needs. According to Procurement and Finance staff, duplicate vendors are occasionally needed due to a combination of the need to track payments, PeopleSoft limitations, and the ancillary systems (Origami, TXbase, and WAM) that interact with PeopleSoft. Based on the classification, there are fields that do not exist in other classifications which are used to track payment information. Since this information needs to be

---

<sup>10</sup> There are 4885 instances where an address description is missing. The issue was not included in the table since this number is in relation to the number of pages (30,121) in all vendor files and not just the number of vendor files (17,110).

<sup>11</sup> Tueffel, "Boost the Bottom Line with Accounts Payable Best Practices", 2-5.

tracked and all payments need to be made through PeopleSoft, staff chose to create a duplicate vendor file with a different classification. In addition, staff stated that to purchase and pay for products or services using these ancillary systems, the vendor sometimes requires the use of specific vendor information. Unfortunately, these systems can only handle one supplier name/set of vendor information, which may not be the one that gets uploaded from PeopleSoft. Again, staff decided to create a duplicate supplier to work around this limitation, so that the vendor information they need gets uploaded to these other systems.

The data quality issues primarily stem from the lack of awareness of existing documents, multiple methods for data entry, and conflicting statements in the Supplier Entry and Update document about the necessity of entering a TIN/SSN.<sup>12</sup> Specifically, regarding the fields with missing data, PeopleSoft does not force the user to enter in required data when the vendor file is created or updated.

Finally, it is not clearly stated who is responsible for maintaining the documentation used in the process or when the documentation was last reviewed. The Council does not identify system or data owners for the vendor file. Best practices recommend agencies clearly identify who owns internal processes and data.<sup>13,14</sup> This lack of clear roles and responsibilities contributes to the data quality issues and can impact data reliability (**Table 2**).

**Table 2: Typical File Issues**

Issue	Count	Percent of Total
<b>Missing TIN Type</b>	8	.05%
<b>Missing Address</b>	425	2.5%
<b>Blank TIN/String of 9's</b>	244	1.4%
<b>Duplicate Vendors</b>	464	2.7%

Having duplicate vendors increases the likelihood for fraudulent activity and sending erroneous or duplicate payments. Additionally, due to duplicate vendors and inaccurate or missing information in the vendor file, any reporting regarding suppliers out of PeopleSoft may be inaccurate and lead committees or staff to make incorrect decisions.

**Recommendation:**

- Staff should review existing documentation to determine what information is needed in a vendor file, if and when duplicate vendor files are needed, and what the naming conventions should be. Staff should identify process and document owners. These individuals should

---

<sup>12</sup> PeopleSoft Financials: New Supplier Entry and Supplier Updates, pg. 2.  
<sup>13</sup> Olavsrud, Thor. (March 2021). "Data governance: A best practices framework for managing data assets".  
<sup>14</sup> Joe (June 2017). "System Owners and Process Owners: Key Drivers of Improvement".

update and/or create the necessary procedures or work instructions and remove duplicate vendor files as appropriate.

**Management Response:** Management acknowledges that the book of record needs to be complete, accurate and always have consistent data. Documentation of required data such as missing TIN, TIN type and address, etc. must be maintained and applied consistently across the Council. This document will contain the standard way to enter vendor information, so all platforms have the same data. The document must also explain, if need, what are the only reasons why a vendor would be set up in a duplicate manner, and what support must be on file to document the set up.

**Timetable:** Documentation of a new Policy and Procedure to be completed by January 2023. The PeopleSoft Business Systems Team will run a report identifying duplicate Procurement supplier entries and provide a report to Procurement Vendor Maintenance staff. Staff will review and delete duplicate suppliers where appropriate by the end of Q4 2022.

**Staff Responsible:** Marie Henderson, Deputy CFO and Jody Jacoby, Director of Contracts and Procurement will co-lead this effort. Staff responsible for the new policy and procedure will be assigned Procurement staff; Tammy Prigge, HRA; and Amanda Martens, Risk

**Audit Follow-Up:** Confirmation and Retest.

### **Procurement staff may manually enter the same vendor information up to three times per entry.**

Procurement staff must manually enter vendor information into the Council's purchasing systems, WAM and TXbase because the purchasing systems do not fully communicate with PeopleSoft. If a vendor serves both Metropolitan Council Environmental Services and Metro Transit, Procurement staff must enter the same information three times. Once in PeopleSoft, once in TXbase, and once more in WAM. This triple entry slows down vendor entry and forces the Vendor Managers to spend more time on data entry instead of their other duties. This is an inefficient use of resources. Furthermore, additional entry creates more opportunities for data entry errors, which in turn creates inaccurate vendor profiles and negatively affects data reliability.

For TXbase, the vendor's Tax Identification Number (TIN), address, e-mail, payment terms, and most contact information is not successfully migrated PeopleSoft to the purchasing systems. For WAM, vendors' contact information, address, e-mail, currency, and payment terms are not pulled over. Additionally, this information is not reviewed once it is entered into the purchasing systems as vendor information is only reviewed when it is entered into PeopleSoft. Failing to review information in the purchasing system increases fraud opportunities as staff could (inadvertently or purposefully) modify key information.

#### **Recommendation:**

5. During the BPSI project, vendor managers from Risk Management, Housing Redevelopment Authority, and Procurement should meet with the integrator to ensure that their needs are met. Some needs could be ensuring proper data migration, validating redundant files, automated vendor inactivation, and an automated, periodic review of vendor information.

**Management Response:** Management acknowledges there are inefficiencies with the current systems the Council maintains for vendor set up. A policy with procedures will be documented as noted.

Long-term solution will be to have one system for vendor set up. This will need to be evaluated with the BPSI project, because currently vendor set up in Risk Management (Origami) and HRA (Happy) are not in scope for this project. The current process is information is entered into PeopleSoft and then synchronized with Origami and Happy.

**Timetable:** Documentation of a new Policy and Procedure completed by January 2023.

**Staff Responsible:** Marie Henderson, Deputy CFO and Jody Jacoby, Director of Contracts and Procurement will co-lead this effort. Staff responsible for the new policy and procedure will be assigned Procurement staff; Tammy Prigge, HRA; and Amanda Martens, Risk.

**Audit Follow-Up:** Confirmation

### The vendor file audit log is unreviewed.

In line with best practices, the Council's system of record has an audit log for changes made to vendor files. This log identifies who made the change and what the change was. For example, if a vendor manager changes a vendor's bank account or address, the log records the date, user, and change. However, management does not review the audit log.<sup>15</sup> Management was unaware that Risk Management and HRA staff can edit information in PeopleSoft. By failing to review the audit log, unauthorized personnel could make changes to the vendor file without alerting management. Likewise, authorized personnel could make inappropriate changes to vendor files without alerting management. Given the sheer number of transactions, it is unreasonable to expect the Controller to be able to effectively review this file for fraud or suspicious transactions manually.<sup>16</sup>

Regularly reviewing the audit log is a fraud monitoring tool and can help ensure that vendor setup rules are consistently followed. The vendor audit file is commonly tested in vendor management audits.<sup>17, 18</sup>

### Recommendation:

6. Management should use the audit log as a control for the vendor file and design a documented control in line with proper segregation of duties and current best practices.

---

<sup>15</sup> Management reviews "Superusers" for the Office of the State Auditor. "Superusers" are a group of users with a specific role in PeopleSoft. They are "users that have the ability to make additions or changes to specific records within PeopleSoft Financials that may impact the validity of the entered data." According to the source document, there are 21 superusers. This report is not a control on the vendor file.

<sup>16</sup> In a one-month span, there were nearly 850 vendor changes. Audit tested only changes made to vendors and did not include the transactions of additional Super Users.

<sup>17</sup> Oseguera, J. and Bashaw, L. (December 2015). "Audit of the City's Master Vendor File." The City of Sacramento, California.

<sup>18</sup> BKD, LLP. (September 2018). "The Consolidated City of Indianapolis and Marion County Vendor Master File Assessment."

**Management Response:**

Management agrees that audit logs in the system are important for review of data integrity, forensic analysis, and transactional review. Periodic review of the system logs should be completed. Management will review a segregation of duties matrix and set up a review process that will ensure that a control is in place.

**Timetable:** End of Q1 2023

**Staff Responsible:** Marie Henderson, Deputy CFO

**Audit Follow-Up:** Confirmation.

**Staff do not check for conflicts of interest.**

There were employees that shared addresses with active vendors in the supplier and HRA files. The Council's Conflict of Interest Policy prohibits the Council from entering contracts where an employee may indirectly or directly benefit.<sup>19</sup> Additionally, Council employee salaries should exceed the income limits for housing assistance under the Family Affordable Housing Program.<sup>20</sup>

Staff do not check for vendor conflicts of interest prior to interacting with a vendor. Instead, they rely on the vendors to self-certify that they do not have a conflict. The self-verification is not verified. There is not a point in the pre-award process where staff check for undisclosed conflicts of interest. The only vendor verification staff perform is to confirm if a TIN currently exists. Additionally, the Council does not perform periodic reviews of the vendor file to identify conflicts that arise during a contract. Council staff are currently updating the Council's guidelines on conflicts of interest in procurements and the Council's Conflict of Interest procedure.

This issue poses financial, operational, and reputational risks to the Council. By not checking to determine if an employee has an interest in a company, it gives the appearance that the Council is irresponsible with public money. Additionally, it gives the appearance that employees have an advantage in procurements, thus eroding the public's trust. Furthermore, failing to check for conflicts could allow an employee to "double dip" by being paid by the Council for contracted work and their regular job duties. Finally, Council employees receiving housing assistance is potentially fraudulent and prevents others from receiving housing assistance.

Management has been informed of any potential conflicts of interest.

**Recommendations:**

7. Procurement and HRA should identify indicators for fraud and conflicts of interest and regularly test them. This could involve creating an exception report for matching vendor and employee

---

<sup>19</sup> Ibid. "The Council shall not enter into any contract or purchase order for goods or services in which a Council Member or a Council employee has an indirect or direct personal financial interest or will personally benefit financially from the contract or purchase order."

<sup>20</sup> Family Affordable Housing Program. "FAHP placement is limited to families with incomes at or below 50% of the area median income."



information. The control should consider data privacy and security. Additionally, Finance, Procurement, and HRA should create a tool and policy to proactively identify conflicts.

**Management Response:**

Management acknowledges that conflict of interests should be reviewed when setting up a vendor. During the vendor set up, it should be verified if the vendor is an employee.

If an employee, extra verifications should take place and documented. For example, what is the vendor request for? HRA would have a conflict of interest if an employee is also a landlord. However, Risk would not, if the payment was to a current employee for a workers' compensation claim or property damage claim.

Employees may also work or have a vested interest in a business/company we pay for claim purposes by are legally obligated to pay.

It will be key in the documentation and procedure, when setting up an employee as a vendor all areas of conflicts are documented, and action taken.

An updated conflict of interest policy will help guide the correct steps when setting up an employee as a vendor

**Timetable:** Documentation of a new Policy and Procedure completed by January 2023. Updates to the Conflict-of-Interest Policy will be completed by the end of Q4 2022.

**Staff Responsible:** Marie Henderson, Deputy CFO and Jody Jacoby, Director of Contracts and Procurement will co-lead this effort. Staff responsible for the new policy and procedure will be assigned Procurement staff; Tammy Prigge, HRA; and Amanda Martens, Risk Staff responsible for the updates to the Conflict-of-interest procedure will be assigned Procurement staff.

**Audit Follow-Up:** Confirmation.

- 8. Procurement, Finance, Human Resources, and Audit should work together to create and implement a conflict-of-interest training.

**Management Response:** Management agrees the conflict-of-interest policy and training should be given to all staff, as a refresher on this important topic.

**Timetable:** Training for all staff should be completed by end of quarter 1, 2023 (March 31, 2023)

**Staff Responsible:** Assigned Procurement staff will work with LOD, as appropriate to create a training specific to conflicts of interest in the procurement process.

**Audit Follow-Up:** Confirmation.

**Private and confidential data was available in internal systems.**

Certain vendor information was improperly made available on SharePoint as part of the New Vendor Request Form and in the Council's purchasing systems, TXbase and Work and Asset Management (WAM). Under the Council's Data Practices Procedure, not public data should only be accessible to



persons whose work assignment reasonably requires access to the data.<sup>21</sup> Some of the data made available is classified as private, confidential, and private and confidential under the Metropolitan Council's Data Practices and Access Procedure.<sup>22</sup> Audit followed up with several stakeholders to verify if there was a business reason this information should be broadly available. Only one stakeholder identified a potential business need while all others stated the information could be removed. Audit believes the data security risks outweigh the objection.

For the SharePoint portal, the SharePoint architect did not properly mask protected data from all users. The site administrators mistakenly thought that the site hid all information requests other than an employee's own request. Instead, it was available to anyone who accessed the site.

For TXbase and WAM, there was not a definitive reason why this information was made available. Access to WAM and TXbase's Vendor Master Form was given out at common permission levels. The information is either pulled from PeopleSoft or manually entered by the Vendor Managers. The information is only necessary for Finance operations.

By making this data available, the Council erodes vendors' trust that they will properly safeguard their private and confidential information. It can make vendors more resistant to providing this information at a critical time when the Council is trying to switch away from physical payments. Additionally, the Council has substantially increased its risk of a security breach by making this information available to common permission roles. Any compromised account could acquire and misuse this private information for any active vendor.

#### **Recommendations:**

9. Council staff should take measures to mask private and confidential information in WAM, TXbase, and SharePoint, and only make it available to those who directly need access. Staff should review their databases to determine if there is additional information that should be masked.

**Management Response:** Management agrees that every measure should be taken to safeguard private and confidential information. Systems should be reviewed on who has access to SharePoint, WAM, TXbase, Origami and Happy. This review should include who can see this private and confidential data and why. Access should be removed from anyone that has access to this data and should not. In addition, SharePoint data, WAM and TXbase confidential information is masked.

The following steps have been taken: Confidential data is now masked on SharePoint. Tax identification number is no longer viewable in WAM vendor profiles. Tax identification numbers are removed in TX-Base (completed July 20, 2022). Procurement will collaborate with Data Practices Office to review databases to ensure no additional private information is available and receive training. In addition, roles within Peoplesoft have been set for security permissions to help safeguard data and user access is reviewed yearly.

**Timetable:** Protecting private data was completed July 2022

**Staff Responsible:** Jody Jacoby, Director; and assigned Procurement staff.

---

<sup>21</sup> TECH 3-2a Data Practices Procedure: Access to and Security of Not Public Data.

<sup>22</sup> Metropolitan Council Data Practices and Access Procedure.

**Audit Follow-Up:** Confirmation.

10. All staff involved in vendor creation and maintenance should receive training on data classification, including how to identify potential data breaches.

**Management Response:** Management agrees that policies, procedures, and training should all be completed now, with current systems and in the future with any new systems. Fraud training should be reviewed by all financial staff on a yearly basis. The training should be Council-wide. The Data Practices Office will help provide Council-wide training on data classifications and how to identify potential data breaches.

**Timetable:** Training to be completed yearly, and the first one completed by December 31, 2022.

**Staff Responsible:** *Program Evaluation and Audit will work with stakeholders to identify training opportunities.*

**Audit Follow-Up:** Confirmation

## Conclusions

The Council's methods to create, update, and maintain vendor files is inefficient, does not always follow industry best practices, and is not consistently followed. By implementing better and additional controls the Council will reduce its risk of fraud by reducing the number of duplicate vendor files, having complete and accurate data in the vendor files, testing for conflicts of interest, and removing unused vendor files. The Council can also save money by removing or significantly reducing the duplicative processes that exist. This process illustrates the redundancies, inefficiencies and inaccuracies that result from maintaining multiple systems for purchasing.

The overall process is inefficient and prone to data entry errors due to having at least five different systems that are used to manage vendor information. Each system requires staff to integrate it with the main financial system, approvers, and support staff to maintain the connections. Redundant and inefficient systems are common to Council financial systems. As Council leaders consider new financial systems and the consolidation and integration of current ones, there will be additional opportunities to create improved processes. Implementation of the recommendations in this report is important to mitigate risk in the short term, but careful planning for the longer term will provide opportunities better streamline and integrate systems to reduce risk and improve outcomes.



October 12, 2022

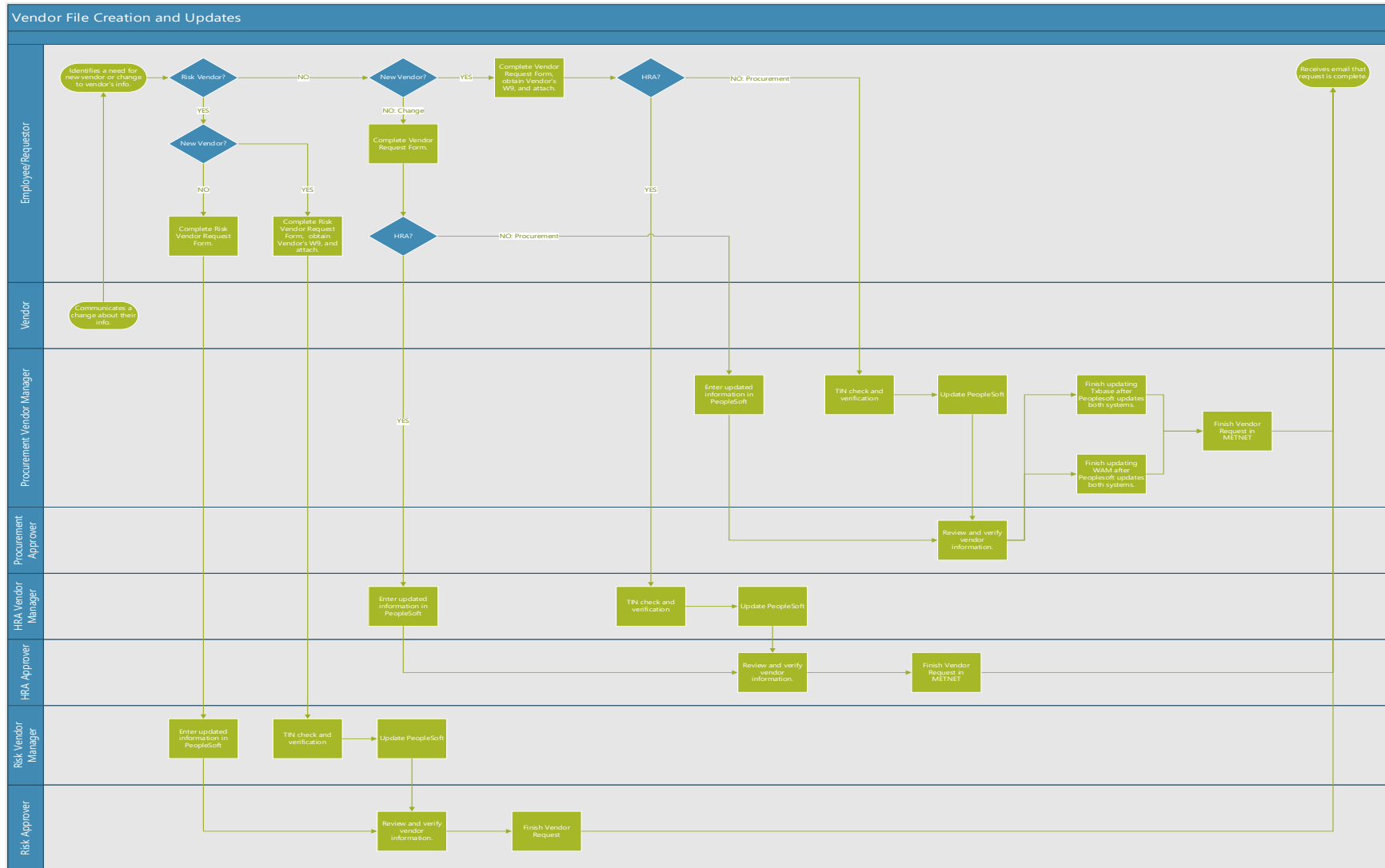
Matthew J. LaTour, Director Program Evaluation & Audit  
Chief Audit Executive

## 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.

# Appendix B



## Distribution List

All audit reports are reported to the general public and are available on [www.metrocouncil.org](http://www.metrocouncil.org). This audit report was distributed to the following parties:

- Members of the Audit Committee
- Regional Administrator
- Deputy Regional Administrator and Chief Financial Officer
- Deputy Chief Financial Officer
- Enterprise Risk Officer
- Director, Procurement
- Manager, Housing Redevelopment Authority
- Manager, Administrative Systems Support
- Manger, Vendors
- Supervisor, Accounts Payable and Receivable



390 Robert Street North  
Saint Paul, MN 55101-1805

651.602.1000  
TTY 651.291.0904  
[public.info@metc.state.mn.us](mailto:public.info@metc.state.mn.us)  
[metro council.org](http://metro council.org)