# INTERNAL AUDIT REPORT

## Vendor Master File Audit

**May 2022**

**INTERNAL AUDIT REPORT**

**VENDOR MASTER FILE AUDIT**

---

**CONCLUSION AND SUMMARY**

This audit has raised significant concerns over the administration and oversight of the vendor master file, which increases the risk of misappropriation and reputational damage to the City. While management has addressed some of the issues identified in the February 2013 Accounts Payable Audit, risks related to system access, incompatible duties and policies and procedures remain.

This conclusion is based on several factors, including:

- Continued existence of employees with incompatible system access and duties.

- The absence of appropriate management oversight over the vendor master file.

- Procurement practices which has had an unfavorable impact on the quantity and quality of vendors in the vendor master file.

- A heavy reliance on manual processes.

- The absence of a complete set of policies and procedures outlining stakeholder roles, responsibilities and accountability over vendor master file related processes and activities.

The following improvements are required:

- Enhance controls over system access control and user access.

- Segregate incompatible duties.

- Ensure the Low Dollar Procurement Module (LDM) is only used if other procurement options are not operationally feasible.

- Deactivate dormant and duplicate vendors on a regular and consistent basis.

- Leverage advances in technology to improve business processes.

- Develop clear and sufficiently detailed policies, procedures and guidelines while providing clarity on roles, responsibilities and expectations of stakeholders as it relates to administration and oversight of the vendor master file.

Depending on how a good or service was procured, staff from Procurement Services or Financial Services could be responsible for creating a new vendor in the vendor master file. Financial Services management are responsible for the administration and oversight of the vendor master file, including activities such as updating and deactivating vendor records. There are various user roles within JDE that allow staff to perform specific tasks within the vendor master file.

The audit confirmed that incompatible system access and incompatible duties continues to be an issue. User access is not reviewed on a regular basis to ensure the number of users and their

level of permission is in alignment with their responsibilities.  Ensuring user access is appropriate is a critical management administration and oversight function as it can mitigate the risk of unauthorized staff adding vendors or changing data on existing vendors and prevents any one person involved in the procure to pay cycle from creating a vendor and applying payment to the same vendor.

Four management employees have the ability to add, change or delete vendor information, enter a vendor invoice into the system for payment, approve a vendor setup or change, and deactivate or reactive vendors.  Although a Payee Control function was implemented within JDE in 2017 that would prevent these four employees from printing cheques, they have the authority to direct the work of the staff who have the ability to print cheques, which would allow these four employees the opportunity to override this system control.   As a compensating measure, the Accounts Payable Supervisor is required to review and approve cheque batches prior to payment.  According to the Supervisor of Accounts Payable, these four employees have never processed a cheque batch before and it would be a flag for her to elevate it to one of the other management members if it were to occur.

Moving the responsibility and accountability of vendor master file "V" type vendor file management, including creating new vendors, amending existing vendors, reactivating dormant vendors and vendor related approvals, from Financial Services to Procurement Services, would effectively segregate vendor procurement and payment duties (the responsibility for the other vendor types will remain with Financial Services).

The 2013 audit identified that the vendor master file consisted of approximately 20,000 vendors, of which 80% were for one-off purchases of less than $3,000.  Management assumed at that time that the introduction of the Purchasing Card (P-Card) program would reduce the number of low value purchases going through Accounts Payable and decrease the number of vendors in the vendor master file.

Although the P-Card program was launched as anticipated, the number of vendors contained in the vendor master file has grown to 34,499 active records, as of December 2020.   A disproportionate amount of City resources are being consumed in the processing of Low Dollar Value (LDM) payments.  A vendor record needs to be created for each one of these vendors. There are excessive administrative costs in managing a larger than necessary vendor master file and processing excessive cheque payments.  There is also increased risks of human error in processing invoices, increased invoice processing times, not taking advantage of potential early payment discounts and increased risk of misappropriation.

Minimizing the use of LDM's and transitioning these types of purchases to competitive procurement processes, establishing additional vendors of record, and ensuring one-off purchases are paid via P-Cards, would reduce the number of active vendors in the vendor master file and mitigate these risks.  It would also free up resources in the Financial Services department to focus on more value-added activities.

To maintain an accurate vendor master file, dormant vendors need to be deactivated in a timely manner.  This is a common internal control used to prevent fraudulent or erroneous payments from being processed.  By deactivating dormant vendors, the vendor master file is easier to

manage, records are easier to access, and processing times may be reduced.  The presence of duplicate vendors can increase the risk of duplicate payments and fraudulent activity and can hamper management's ability to perform vendor specific spend analysis.  The Office of the Chief Information Officer (OCIO) developed a vendor master file clean-up process but issues were identified in the design and operating effectiveness of the process.  This includes using three years of inactivity rather than two to perform the cleanup, manually reviewing each vendor prior to deactivating, and not running the query on each vendor category.  The result is consistent with the number of dormant and duplicate vendor records and incomplete data that was observed in the vendor master file.  This risk is amplified when clearly defined policies, procedures and review processes do not exist to ensure vendor information is correctly and consistently entered.

The audit identified opportunities to better leverage technology to improve business processes. This includes automating the vendor deactivation process using the tool developed by the Office of the Chief Information Officer (OCIO).  The creation of additional types of management reports, such as a vendor reactivation report, would assist management in performing their oversight responsibilities.  Several manual processes were also observed.  Management should explore the use of automated workflows to increase the efficiency and effectiveness of many of these processes.  Management, with Council support, should continue to explore how integrating technology with business processes can improve the way we deliver service and enhance our ability to obtain usable data for analysis, management reporting and informed decision making.

The 2013 audit identified that there were no documented procedures that outline the processes or provide guidelines supporting the payment process cycle.  This audit confirmed that workflow diagrams have recently been created that outline stakeholder roles and responsibilities for some vendor master file processes.  In addition, some process narratives have also been developed that may be useful job aids for staff who are already familiar with the process.  However, for anyone new stepping into the role or anyone unfamiliar with the process, it would not be clear who is responsible for performing the narrative tasks and there are no sections outlining management's oversight role and accountability over these processes.

Clearly and sufficiently detailed policy and procedures providing clarity and guidance on roles, responsibilities and expectations of stakeholders as it relates to administration and oversight of the vendor master file need to be developed, using the City's approved Policy and Procedure templates.  Documenting policies and procedures are a key control because these documents help to promote consistency among staff and can be used to reinforce compliance, manage risk, and used as a training mechanism for new staff.  The impacts of the absence of these documents were evident through all aspects of the audit.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

Internal Audit will follow up on the status of outstanding management action plans related to this audit and will report the status to a future Audit Committee meeting.

## BACKGROUND

The vendor master file is fundamental to the appropriate functioning of the City's procure to pay process.  The vendor master file is a database which houses key business information about City vendors such as the vendor's name, mailing address, tax identification and vendor type.  The information is maintained in the City's JD Edwards (JDE) software, including scanned copies of vendor information provided by departments to Financial Services as part of vendor additions and information changes.  The information is utilized to facilitate payments and transactions to vendors as part of the procurement of goods and services.

The vendor master file is also used to facilitate employee expense reimbursements, refunds to property tax owners who made tax overpayments, election rebates, recreation refunds, permit refunds, citation and bylaw refunds, Vaughan Business Enterprise Centre Starter Company Plus Program grants, and other one-time type payments.

As of December 31, 2020, the vendor master file contained 34,499 active records.

The effective maintenance of the vendor master file is critical to mitigating against unauthorized or inappropriate payments, prevention of duplicate transactions, and to reduce inefficiencies. Inaccurate, incomplete, unauthorized or duplicate vendor records could adversely impact the processing of vendor payments and/or may increase the risk and likelihood of vendor related fraud.

**INTERNAL AUDIT REPORT**

**VENDOR MASTER FILE AUDIT**

---

**OBJECTIVES AND SCOPE**

The objective of this audit was to evaluate the adequacy and effectiveness of the internal controls, processes and procedures related to the vendor master file, and that they are adequately designed, established and operating as intended to mitigate business risks associated with the City's procure to pay processes.

The audit scope included assessing that:

- Adequate policies, processes and procedures exist for new vendor validation, set up, modification and maintenance of vendors in the master file and are regularly reviewed, updated, and applied consistently.

- Access to the vendor master file is appropriately secured, safeguarded and restricted to authorized individuals, including adequate segregation of duties.

- Data entered into the vendor master file is complete, accurate and valid.

- There is adequate management oversight, ensuring appropriate administration and supervision of the vendor master file.

- Inactive and duplicate vendors are identified, assessed and deactivated on a regular and consistent basis.

- Information Technology systems are being effectively leveraged and used to their maximum capabilities.

The audit scope included vendor master file records and transactions in JDE between January 1, 2019 – December 31, 2020.

This audit was conducted in conformance with the *International Standards for the Professional Practice of Internal Auditing.*

**Auditor and Author:** **Luca DeFazio, CPA, CA**

**Director and Author:** **Kevin Shapiro CIA, CFE, CRMA**

**INTERNAL AUDIT REPORT**

<u>**VENDOR MASTER FILE AUDIT**</u>

---

<u>**DETAILED REPORT**</u>

### 1. *Enhance Controls over System User Access and Segregate Incompatible Duties*

The most widely accepted model for explaining why "good people" commit fraud is the Fraud Triangle, developed by Dr. Donald Cressey. According to the model, there are three factors that increase the risk of an ordinary person committing fraud. All three of these factors must be present at the same time for fraud to occur. These factors include Pressure, Perceived Opportunity, and Rationalization[1]. Therefore, it is crucial that as part of financial system control design, the risk of an opportunity to commit fraud must be appropriately mitigated. Ensuring appropriate system access and segregating duties are the most common internal controls to mitigate opportunities to commit financial related fraud.

Segregation of duties is a vital element of any control system and should be designed in a way that limits an employee's ability to perform incompatible or unnecessary tasks. It's the act of splitting tasks among employees to reduce the opportunity of one employee committing fraud. When segregation of duties is not possible, management must implement compensating controls to mitigate the risk.

According to the Information Systems and Control Association (ISACA), system access should be granted on a "need-to-know" basis when there is a legitimate business requirement to have access.

The Institute of Internal Auditor's (IIA) Global Technology Audit Guide on Identity and Access Management (GTAG 9) states that "As part of its Identity and Access Management monitoring process, the organization should establish a methodology to periodically review the access rights granted to all identities residing in its IT environment."

***An Accounts Payable Audit, presented to the Finance, Administration and Audit Committee in February 2013, identified several issues as it relates to unnecessary and incompatible access to the vendor master file. This audit confirmed that management has still not adequately addressed these risks.***

There is sufficient, reliable, relevant and useful evidence to support that Financial Services Management does not have appropriate controls in place to ensure that staff are assigned appropriate system access based on their current day-to-day job duties. This evidence includes:

- The absence of formalized policies and procedures outlining roles, responsibilities and accountability for management administration and oversight over system access.
- Periodic reviews of system access privileges are not performed to ensure user access remains necessary and appropriate based on current job duties.
- Numerous employees have multiple User ID's and inappropriate User Roles.
- Inactive employees have active JDE user access.

---

[1] Further information about Fraud and the Fraud Triangle can be found at: <u>Fraud 101: What is Fraud? (acfe.com)</u>

- According to Financial Services Management, a cleanup of system user roles was performed a few years ago. However, the Controller was unaware that many staff still had the ability to perform system tasks that they should not be able to perform. This includes:
  - 6 staff having the ability to add, change or delete vendor information, while at the same time having the ability to enter AP invoices, create cheques, have access to cheque stock, and access to cheques before they are mailed out.
  - 48 employees across the City have the ability to reactivate vendors and no clear explanation was provided as to why so many employees require this access.

Four management employees have the ability to add, change or delete vendor information, enter a vendor invoice into the system for payment, approve a vendor setup or change, and deactivate or reactive vendors. Although a Payee Control function was implemented within JDE in 2017 that would prevent these four employees from printing cheques, they have the authority to direct the work of the staff who have the ability to print cheques, which would allow these four employees the opportunity to override this system control. As a compensating measure, the Accounts Payable Supervisor is required to review and approve cheque batches prior to payment. According to the Supervisor of Accounts Payable, these four employees have never processed a cheque batch before and it would be a flag for her to elevate it to one of the other management members if it were to occur.

For new vendors added through a competitive process, the Procurement System Specialist creates the vendor in the system and performs the vendor validation. Financial Services approves the vendor set up by Procurement in JDE before any payments can be processed.

Other system access issues that were noted include:

- The Accounts Payable Supervisor has the ability to add, change or delete vendor information, enter a vendor invoice in A/P, create cheques, access to cheque stock, access to cheques before they are mailed out, deactivate or reactivate vendors. However, the Accounts Payable Supervisor does not have the ability to approve vendor additions, changes or deletions, and payments cannot be processed until vendor additions and changes are approved by the Senior Financial Analyst, Assistant Controller or Controller.
- Both the Controller and Assistant Controller have made vendor information changes and approved their own changes. According to the Controller, it is more efficient for them to make minor corrections, such as to correct vendor name or address spelling errors rather than to hold up the process by making the person who made the error correct it.

In our yearly Internal Audit Annual Report, we include a section about the Institute of Internal Auditors Three Lines Model. It outlines the roles of various leaders within an organization, including oversight by the board or governing body, management and operational leaders including risk and compliance (first and second-line roles), independent assurance through internal audit (third line) and it addresses the position of external assurance providers. The model applies to all organizations, regardless of size or complexity. Concepts of this model

are routinely shared and discussed by Internal Audit with the SLT-E team, and how they can be applied at the City.

Second line roles may include monitoring, advice, guidance, testing, analyzing, and reporting on matters related to the management of risk. Insofar as these provide support and challenge to those with first line roles and are integral to management decisions and actions, second line roles are part of management's responsibilities and are never fully independent from management, regardless of reporting lines and accountabilities[2].

In the procure to pay cycle, OCIO staff should be assuming a second line role to ensure that the first line do not have the capability to circumvent controls through the JDE system[3]. OCIO staff do not question or challenge Financial Services Management when they request user role additions, changes or modifications, even if the request would allow a user to have access that is not needed for their role or be incompatible with other duties. Based on discussions with OCIO staff, they have never been asked to assume this second line role, nor do they have a sufficient level of operational understanding of the procure to pay cycle to perform this oversight function.

The absence of controls over employee access rights and incompatible duties has significantly increased the risk of misappropriation and reputational risk to the City.

### Recommendations

We recommend that management:

- Move the responsibility and accountability of vendor master file "V" type vendor file management, including creating new vendors, amending existing vendors, reactivating dormant vendors and vendor related approvals, from Financial Services to Procurement Services, to effectively segregate vendor procurement and payment duties (the responsibility for the other vendor types will remain with Financial Services).

- Perform a comprehensive review of existing system user access rights to ensure, that at minimum:
    - Only active employees with legitimate business requirements have access to the JDE system, including the vendor master file, and their access is based on their current job duties. This includes removing the access of employees who are on long term leaves of absence, such as medical and parental leaves.
    - Incompatible access rights are removed from employee/job profiles. This includes at minimum, removing the inappropriate access from the four Financial Services Management staff and the Supervisor, Accounts Payable. Financial Services Management staff should only have review and approval access.
    - Vendor reactivation access is restricted to only those employee(s) who need to perform the task.

---

[2] Extract from The IIA's Three Lines Model: An Update of the Three Lines of Defence
3 The principle of least privilege (POLP) is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities.

- Ensure that system access reviews are performed at minimum, annually.

- Develop clearly documented policies and procedures outlining roles, responsibility and accountability as it relates to the management and oversight of the vendor master file, including appropriate user access.  In addition, these policies and procedures should be completed on the City's Policy and Procedure templates, approved for use by the City's Policy Committee.

- Develop and implement a strategy to incorporate the IIA's Three Lines Model, specifically the second line role within OCIO, that at minimum, would give OCIO staff the knowledge and responsibility to challenge and elevate concerns regarding incompatible and inappropriate system access to higher levels of management for appropriate remediation.

**Management Action Plan**

Management agrees with the audit recommendations.

Responsibility over Vendor File Management

On December 10th, Council approved a corporate reorganization which included moving the Procurement Services department from the Corporate Services portfolio to the Administrative Services portfolio.  This change will help facilitate the segregation of procurement activities from payment activities.  As part of this transition, responsibility and accountability over the "V" the type Vendors in the vendor file will transition to Procurement Services.

Procurement Services will be responsible for the management and maintenance of "V" type vendors in the Vendor Master file, including creating new "V" type vendors, amending existing vendors, reactivating dormant vendors and vendor related approvals.  Financial Services will continue to be responsible for the management and maintenance of all other vendor types in the Vendor Master File.  Financial Services will continue to be responsible for processing all payments.

Procurement Services and Financial Services are currently in the process of onboarding new Directors.  Moving the type "V" vendor  VMF responsibilities to Procurement Services will require additional resource support with the appropriate knowledge, experience, and skillset to transition seamlessly and without any adverse operational impacts and minimal disruption to operations.

There will be a transition period as Procurement Services, Financial Services and OCIO finalize the details of the change.  The implementation date for the completion of this transition will be Q4 2023.

User access rights

JD Edwards access rights need to be reviewed and modified to provide a more appropriate segregation of duties in the JD Edwards system.  Known required changes will be made immediately.  Procurement Services and Financial Services will perform a comprehensive review of current JD Edwards roles with OCIO and develop the appropriate roles that provide the appropriate access for all users by the end of Q4 2023.  Through this review we will ensure that

only active employees with legitimate business requirements have access to the JDE system, including the vendor master file, and their access is based on their current job duties. This review will ensure that incompatible access rights are removed from employee/job profiles. This includes at minimum, removing the inappropriate access from the four Financial Services Management staff and the Supervisor, Accounts Payable. This also includes removing the access of employees who are on long term leaves of absence, such as medical and parental leaves.

Once the above user access changes have been made, Financial Services, Procurement Services and OCIO will implement an annual review of access rights with respect to the Vendor Master File.

While this recommendation states access to the entire JD Edwards enterprise reporting system (JDE), we do believe this to be a more extensive exercise and will work with the Office of the Chief Information Officer (OCIO) to review. There is currently a corporate program of Finance Modernization and security will be reviewed through this process as well.

Policies and procedures

In the 2013 audit, it was recommended "to develop written procedures that support vendor management and the accounts payable process cycle". Based on that recommendation, detailed written procedures based on the process were developed. Based on the current audit recommendation, Procurement Services and Financial Services agree to create policies and procedures and ensure they are in the current format for the City's policies and procedures templates for each of their respective responsibilities for the Vendor Master File. Management will review these new policies and procedures with Internal Audit before going through the Administrative Policy Committee for approval. This will be completed by Q4 2023.

Three Lines Model

Based on the comprehensive review of system access that we will be conducting, access rights will be linked to specific responsibilities. Management will be developing a system access responsibility matrix by position. Any changes to this matrix will need the approval of both the DCM of Administrative Services and the DCM of Corporate Services, City Treasurer and CFO. This work can be completed by OCIO submitting a ARR resource request in 2023 for a JDE Security officer who can hold these responsibilities.

In addition, the Office of the Chief Human Resources Officer will be responsible for communicating changes to employee status so that OCIO can update system access accordingly. This will be completed by Q4 2023.

2. ***Enhance Processes and Controls over the Management, Administration and Oversight of the Vendor Master File Data***

The 2013 Accounts Payable Audit identified that management was not regularly reviewing the vendor master file for inactive vendors and that changes to the vendor master file were not being monitored.  The 2013 audit also identified that there were no documented procedures that outline the processes or provide guidelines supporting the payment process cycle.  Internal Audit has reviewed the vendor master file data and the processes management has implemented since the 2013 audit and noted the following:

- This audit confirmed that workflow diagrams have recently been created that outline stakeholder roles and responsibilities for some vendor master file processes.  In addition, some process narratives have also been developed that may be useful job aids for staff who are already familiar with the process.  However, for anyone new stepping into the role or anyone unfamiliar with the process, it would not be clear who is responsible for performing the tasks and there are no sections outlining management's oversight role and accountability over these processes.  In addition, these documents have not been created using the City's approved Policy and Procedure templates.

- It was also noted that there were several processes not documented, including, but not limited to:
  - Critical data elements that must be included for creating a vendor, including standard naming conventions, vendor creation date, syntax and punctuation.
  - Approach for consistent address, postal code and HST tax ID conventions.
  - Frequency, timing, approach and oversight over deactivating dormant vendors and performing duplicate vendor checks.
  - Segregation of duties

- With the help of OCIO staff, a tool was developed that allows Financial Services Management to identify and then deactivate dormant and duplicate vendors.  According to the Supervisor of Enterprise Systems, these reports were created to be functional with JDE v9.1.  Both reports were run in September 2017.  Due to a JDE system upgrade to v9.2 that took place in November 2017, the functionality to run these reports was unavailable between November 2017 and July 2019, as they were not compatible with v9.2.  Once the reporting tool was recreated to be compatible with v9.2, the dormant vendor reports were run again in December 2019 and January 2021.  The duplicate vendor report was run again in December 2019.

- Based on the 2013 audit report, it was recommended that management deactivate vendors after two years of inactivity.  However, it is now industry better practice to deactivate vendors with 15-18 months of inactivity.[4]

---

[4] Per the Institute of Finance and Management (IOFM) APP2P Conference on Accounts Payable & Procedure-to-Pay, "15-18 months is a good cut-off, 12 is usually too short".

- The process for running the dormant and duplicate vendor reports is manual and time-consuming, as management reviews each vendor identified by the tool to ensure that the vendor should be deactivated. The Accounts Payable Supervisor runs the report, determines which vendors to deactivate, and performs the inactivation without any further review or approval. This process, including the approach, frequency and timing for the dormant and duplicate vendor clean-up have not been documented.

- For the dormant vendor reports run in both December 2019 and January 2021, management chose the wrong date parameters to run the query. As a result, only vendors who were inactive for 3 years or longer, rather than 2 years or longer, were flagged. In addition, the vendor clean-up performed in December 2019 did not include all vendor types. As a result, vendors that should have been deactivated remain active in the system.

- When the duplicate vendor report was run in December 2019, management ran the duplicate query based on vendor name. However, management did not check for duplicates based on other parameters such as address or HST number. As a result, duplicate vendors based on these parameters were missed.

- One-time payment vendors are not immediately deactivated after payment is made.

- The vendor master file still contains dormant and duplicate vendors, incomplete vendor data and inconsistent naming of vendors.[5] For example:
    - Only 29% of V vendors were actively used in the 2020 calendar year.
    - 78% of vendors (includes all record types which receive payments) are dormant as of December 2020 but have not been made inactive.
    - 43% of V vendors (vendors providing goods or services to the City) are considered dormant as of December 2020 but have not been made inactive.
    - 184 duplicate records were identified.
    - 86 V vendor records contain DO NOT USE or DON'T USE directions in the description or address field.

According to the Controller, one of the reasons why there are so many duplicates is that only one address can be assigned to a vendor. There are several vendors that the City deals with, including government agencies, that have different locations where payments may need to be sent to. Internal Audit and management have confirmed with the vendor that our current system does not have the ability to set vendors up using a "Parent/Child" relationship functionality, which would assign an overarching vendor name and child (the same vendor with different address locations).

In discussions with OCIO staff, it was confirmed that the tool they developed to flag dormant and duplicate vendors could be programmed to run in the background without the need for management intervention. In other words, JDE could be programmed to run a dormant vendor

---

[5] Naming conventions are a set of rules identifying what information needs to be entered and how it needs to be entered to ensure vendor data is accurate and complete. Effective naming conventions help prevent duplicate vendors, reducing the opportunities for duplicate payments.

check on the 1st of every month, which would automatically deactivate any vendor that had not been paid after a user defined period of time.

The longer duplicate and dormant vendors remain in the vendor master file, the larger it becomes. This increases the risk of using incorrect vendors, increased administrative costs of managing a larger population and potentially overlooking fraud.[6] This risk is amplified when clearly defined policies, procedures and review processes do not exist to ensure vendor information is correctly and consistently entered.

**Recommendations**

We recommend that management:

- Develop formalized policy and procedures, using the City's Policy Committee approved templates, which provide guidance as to the creation, management, administration and oversight of vendor master file data. Elements of these documents should include, but not be limited to:
  - Critical data elements that must be included for creating a vendor, including standard naming conventions, vendor creation date, syntax and punctuation.
  - Consistent address, postal code and HST tax ID conventions.
  - Frequency, timing, approach and oversight over deactivating dormant vendors and performing duplicate vendor checks.
  - Segregation of duties

- Use the orchestration tool developed by OCIO staff to automatically deactivate vendors who have not been used (i.e., no payments processed) for the past 18 months, on the first of each month.

- Ensure the duplicate vendor deactivation clean-up process is performed on an annual basis for all vendor types and all duplicate parameters.

- Investigate the feasibility of developing a tool that would deactivate one-time type vendors after the payment is made.

- Modify incorrect and/or incomplete data structures, including filling in blank/ missing fields of all existing active vendors.

---

[6] Journal of Accountancy, *Boost the bottom line with accounts payable best practices*, states that, "The median time of detection for fraud schemes is 18 months, and the longer a fraud lasts, the greater the financial damage it causes… The majority of organizations that fall victim to fraud fail to recover their losses. Those that do screen for risk factors and early warning signs uncover fraud cases more quickly and significantly reduce losses."

---

## Management Action Plan

Management agrees with these recommendations.

Formalized policy and procedures

Procurement Services and Financial Services Management will develop formalized policies and procedures to provide guidance as to the creation, management, administration, and oversight of vendor master file data for which they are respectively responsible.  Elements of these documents will include, but not be limited to:

- Critical data elements that must be included for creating a vendor, including standard naming conventions, vendor creation date, syntax, and punctuation.
- Consistent address, postal code and HST tax ID conventions.
- Frequency, timing, approach and oversight over deactivating dormant vendors and performing duplicate vendor checks.
- Segregation of duties

The policies and procedures will be completed, approved and communicated to all stakeholders by Q4 2023.

Automatic deactivation

OCIO will implement the existing tool to automatically deactivate type "V" vendors who have not been used for the past 18 months for Procurement Services.  OCIO will implement a similar tool for Financial Services for all the other vendor types.  This will be scheduled automatically to run on the 1st of every month, by Q4 2023.

Duplicate Vendor Review Process

Procurement Services and Financial Services will be responsible for performing the duplicate vendor review process for the vendor types they are responsible for.  This will be incorporated into their respective policies and procedures.  The duplicate vendor review will be conducted annually in Q1 as part of our year-end processes.

Deactivating one-time type vendors

OCIO will engage Oracle to investigate if there is existing functionality to perform this task.  Most of the one-time payments are refunds for tax, recreation, and development.  Currently tax and recreation have a separate type in the Vendor Master File.  Management suggests creating a vendor type for development refunds to continue under Financial Services oversight. Procurement Services will update the Vendor Create and Update form for "V" type vendors to include a section for the requesting department to indicate if the vendor will be a one-time vendor. This will be completed by Q4 2023.

**VENDOR MASTER FILE AUDIT**

Modify incorrect and/or incomplete data structures

Critical data elements for creating or updating a vendor, including standard naming conventions, vendor creation date, syntax and punctuation, address, postal code, phone #'s and HST tax ID conventions will be documented in our policies and procedures.  The vendor master file cleanup efforts will reflect these standards.  If there are fields that are intentionally left blank, our policy and procedures will clearly identify these instances and the oversight processes management will be performing to validate the blanks.  This will be completed by Q4 2023.

**3. *Ensure the Low Dollar Procurement Module (LDM) is Only Used If Other Procurement Options are not Operationally Feasible***

The 2013 Accounts Payable Audit identified that the vendor master file consisted of approximately 20,000 vendors, of which 80% were for one-off purchases of less than $3,000. As of December 2020, the number of vendors contained in the vendor master file has grown to 34,499 active records. According to the former Director of Procurement Services, 1,190 LDM new vendors were added to the vendor master file in 2020 compared to 98 through competitive processes.

In 2013, management assumed that the introduction of the Purchasing Card (P-Card) program would reduce the number of low value purchases going through Accounts Payable and decrease the number of vendors in the vendor master file. In all likelihood, this assumption would have held true if the way of procuring low value goods had completely transitioned to the P-Card program.

Prior to the launch of the P-Card program, first as a pilot in June 2013, followed by a full rollout in June 2015, one-off purchases of less than $3,000 dollars were processed as Field Purchase Orders, then later renamed as Low Value Purchases (LVP's). Despite the success of the P-Card program, LVP's were not eliminated. Instead, on April 1st, 2017, LVP's were replaced with the JD Edwards LDM Purchase Order module. It was thought that LDM's would provide flexibly in use and enhance visibility and analytic capability for low dollar transactions.

In 2020, 4,851 LDM invoices were processed. The total procurement cost of these goods and services was approximately $5.2 million. The breakdown of the invoice dollar amounts are below:

| Invoice Amount | # of Invoices |
|---|---|
| $0.00 - $999.99 | 3,422 |
| $1,000 - $1,999.99 | 643 |
| $2,000 - $2,999.99 | 352 |
| $3,000 - $3,999.99 | 197 |
| $4,000 - $5,000.00 | 237 |
| **Total** | **4,851** |

LDM invoices (invoices less than $5,000) contributed to 18% of the total invoices processed by the City but made up only 1.59% of the total dollar value of invoices paid by the City. This represents a disproportionate amount of effort and associated cost required to process the invoices for a very small total dollar value of spend for the City.

*Several audit reports have been presented in the past number of years identifying the need for the City to develop a more proactive and strategic approach to procurement. While efforts have been made by management to reduce both the number of transactions and dollar value processed through LDM's, our analysis of the 2020 LDM data shows that a vast majority of these goods and services could have likely been acquired through either a competitive procurement process or through the P-Card program.*

The 2013 Accounts Payable Audit also recommended that management design reports that would provide preliminary information where competitive bidding and savings opportunities can be further explored. In 2017, Procurement Services developed monthly procurement activity reports, by department, that provides procurement spend data by type and posts them to an internal site.

While Procurement Services has successfully worked with several departments, such as Environmental Services and Facility Management to reduce their LDM purchases, further opportunities exist to analyze procurement spend data on a holistic, corporate wide basis, rather than just at the department level, to identify further opportunities to shift low dollar transactions to more efficient procurement methods.

For example, the audit found several examples of more than one department using the same vendor to make low dollar purchases throughout the year. The highest was 195 invoices with an average invoice amount of $197.47 for a vendor used by both VFRS and Fleet Maintenance Services for automotive supplies.

According to the NAPCP P-Card Value Proposition report, the average cost to process an invoice using a traditional Accounts Payable process is $90 vs. $20 with a P-card. For every invoice payment that is transitioned to a P-card, this could potentially result in an estimated $70 ($90-$20) cost savings to the City. If the City transitioned the total number of LDM invoices to P-card, assuming the quantity of LDM invoices remain consistent, the City can save an estimated $339,570 (4,851 x $70) based on 2020 data. These savings would continue into the future since a permanent transition to P-cards would occur.

There are excessive administrative costs in managing a larger than necessary vendor master file and processing excessive cheque payments. There is also increased risks of human error in processing invoices, increased invoice processing times, not taking advantage of potential early payment discounts and increased risk of misappropriation.

The feasibility of eliminating the LDM module was discussed with the Senior Leadership Team – Executive (SLT-E), on August 17th, 2021. Based on the discussion, the consensus was that it may not be operationally feasible to completely eliminate the LDM module. There could be situations where a low dollar purchase may need to be made when a current contract is not already in place and a vendor does not accept a credit card. In these situations, staff would still need access to the LDM module. It was agreed that SLT-E would work with their staff to ensure that LDM's are only used as a "last resort" and a significant effort would be made to minimize the use of LDM's.

A significant reduction in the use of the LDM process would also free up resources to focus on more value-added activities, as the create a new vendor process is manual and time consuming.

The severity of many of the risks identified in the remainder of this report could be reduced with either the elimination or significant reduction in LDM use.

**Recommendations**

Based on the ongoing risks that have been identified in several audit reports since 2013 and risks identified in this audit, it is recommended that:

- Procurement Services work with client departments to permanently transition LDM procurements to a more efficient and effective procurement method.

- LDM's may only be used for non-recurring operational requirements where the good/service is required immediately and could not have otherwise been obtained via a competitive process or paid using a P-Card.

**Management Action Plan**

Management agrees with these recommendations.

Procurement Services agrees with working with client departments to transition recurring LDM expenditures to a more efficient and effective procurement method.

Following the SLT-E meeting on August 17, 2021, a commitment was made by members of the SLT-E team to review the transactional data provided with their teams and work with Procurement Services to identify more appropriate procurement opportunities.  As a result, the former Director of Procurement Services issued a memo on August 19th to SLT-E and SLT outlining the Low Dollar Module (LDM) Purchase Order Program.  The memo provided a disciplined, four-step approach to identifying further opportunities for shifting low dollar transactions to more efficient procurement methods.

The memo also stresses that LDM's may only be used in a non-recurring, urgent situations where the good/service is required immediately and could not have otherwise been obtained via a competitive process or using a P-Card.

We will seek continuous improvement of reporting standards for LDM's to enable transparency and accountability to lead client departments to a root cause analysis, with the functionality to take corrective actions where appropriate. Specific areas of development will include:
- Web-based interactive dashboard reporting that offers easy access to information which can be summarized at a high level or used to "drill down" into more detail. This level of control enables both high-level strategic views of the LDM's, with the ability to rapidly focus in on areas of concern for more detailed analysis.
- Once information is collated, the reporting team will leverage this capability into building high-level executive dashboards to facilitate quick understanding of the LDM's, and areas

which require a more detailed review. Interactive web-based reports will be built and available for key stakeholders to use on a regular basis.

Since fiscal 2017, Procurement Services has actively worked with client departments by sharing monthly LDM spend trend analysis, providing information to help inform improvement opportunities to significantly reduce the unnecessary use of LDMs and directing the department's procurement needs through appropriate channels, while realizing best value for money for the City through a fair, transparent, and competitive process.   As well, high LDM spend client departments have been addressed through formal memos outlining their spend trends and focusing in areas to redirect spend to alternate procurement methods.   Procurement Services will continue to collaborate with all City client departments to seamlessly transition the departments' low value procurement needs without significantly impacting their operations.

Along with department heads, Procurement Services Staff has been tasked to regularly review and reduce, where appropriate, LDM and P-Card spend by identifying alternate methods of procurement such as Competitive bids, Multiyear contracts, Vendor of Record arrangements and blanket Purchase orders.  With over three years of historical LDM and P-Card data, Procurement Services continues to address the challenges faced by the departments and provide cost-effective solutions to meet their ongoing operational needs.

Both action plans will be fully implemented by Q4 2023.

4. *Enhance Controls over the Vendor Setup and Change Request Process*

Complete, accurate and valid vendor authorization and setup is critical to ensuring the legitimacy and authenticity of vendors in the vendor master file. A common practice is specifying individuals at the department level who have the authority to request vendor setup or information changes via the completion of a vendor setup or change process. Adequate authorization to update the vendor master file is important, in that it:

- Assists in deterring the establishment of fraudulent vendors and disbursement schemes.
- Documents who requested the vendor set up or changes by creating an audit trail. This reduces the risk that requests coming from unauthorized sources are processed and helps to ensure the legitimacy of the request.

Financial Services currently requires a requesting department 'Authorized Signing Authority' to complete a manual Create or Update Vendor form and provide supporting documentation to substantiate a vendor setup or change. The audit identified that the process to update the Authorized Signing Authority SharePoint repository is manual and may add undo complexity to the process.

Automating this process would mitigate risk by ensuring that appropriate authorizations to setup or change vendor information are received, reduce the administrative time circulating forms between the requesting department for review and approval, and improve data quality input into JDE.

It should also be noted that the risk identified in this observation would be significantly reduced by reducing the reliance on LDM procurements. Permanently transitioning these types of procurements to a more efficient and effective procurement method would reduce the number and frequency of new vendor creation requests.

**Recommendations**

We recommend that management investigate the feasibility of automating the new vendor setup and vendor change request processes. This may include developing an integrated online authorization workflow either directly in JDE or via an existing Microsoft platform.

**Management Action Plan**

Management agrees with the recommendation.

In 2016, as a Service Excellence initiative, management removed the process of paper copies of authorized signatories being kept by all Accounts Payable staff. Staff now maintain a central digital copy of this register in SharePoint, which is updated as staff changes occur. This process is necessary to confirm authorized signatures and authorized dollar limits. The authorized signature register, for invoice approvals, is the same used for the LDM process.

In discussions with a JDE vendor of record, they advised that there is no pre-built functionality in JDE to accommodate this. Should this functionality become available, staff will investigate the possibility of implementing it. Other options such as Microsoft will be investigated. This work can

be completed by OCIO submitting a ARR resource request in 2023 for appropriate IT resources including Web, Integration and JDE professional skillsets.  The timelines will depend on the vendor advice after successful procurement.

---

*5.  Enhance Controls over the Vendor Validation Process*

Vendor validation is the process of confirming the legitimacy of the business or person through an external source prior to adding them to or making changes to a vendor master file record. Ensuring the legitimacy of vendors prior to adding them to the vendor master file is a key control because it ensures:

- An independent validation of the legitimacy of new vendors as well as changes to existing vendors by somebody that has no purchasing or payment authorities.
- The accuracy and completeness of vendor or individual details.
- Data quality and consistency.

The audit assessed Financial Services' vendor validation processes and noted the following:

- There are no policy or procedures specifying the appropriate supporting documentation that need to be provided by requesting departments in order to add or make changes to a vendor.  This increases the risk that the type of information submitted to substantiate the existence of a vendor and the process to validate the information is not consistent.

- The Treasury Clerk or Procurement Specialist rely on the requesting department for authenticity of the information provided used to enter into JDE.  The only independent information validation performed by the Treasury Clerk or Procurement Specialist is matching vendor HST number and company's legal name from the invoice to CRA Registry.  Follow-up with the requesting department only occurs if information is incomplete.

In addition to ensuring the legitimacy of a vendor, a thorough validation process helps mitigate the risk of poor data quality which may lead to inefficiencies and creation of incorrect or invalid vendors.  For example, not properly validating a company's legal name could lead to duplicate records.  There is also a risk that by not properly validating vendor information, fictitious or fraudulent vendors can be created.

## Recommendations

We recommend that management:

- Formally define a list of requirements that are required to support and substantiate a new vendor request or changes to an existing vendor and ensure that this information is validated prior to approving the addition or change.

- Develop policy and procedures, using the City's Policy Committee approved templates, defining the roles, responsibility and accountability of all stakeholders involved in the vendor validation process.  The requirements to substantiate new vendors or changes to existing vendors should be included in these documents.

## Management Action Plan

Management agrees with these recommendations.

Procurement Services will formally communicate what departments are required to submit in order to process a new vendor request or change to an existing vendor. This information, along with the associated forms will be made available on VOL. This will be completed by Q4, 2023.

Procurement Services will develop policy and update procedures which will define the roles, responsibility and accountability of all stakeholders involved in the vendor validation process and the requirements to substantiate new vendors or changes to existing vendors. This will be completed by Q4, 2023.

### 6. *Enhance Controls over the Vendor Reactivation Process*

On occasion, vendors who have been deactivated may need to be reactivated. Acceptable occurrences could include vendors who had previously completed a contract with the City who years later, are the successful bidder on a new procurement opportunity. It is critical that effective controls exist to safeguard access to vendor reactivation and that the process is efficiently designed and operating effectively.

The Accounts Payable Supervisor is responsible for reactivating vendors. For deactivated vendors last paid greater than 5 years from the date of reactivation request, the requesting department needs to follow the new vendor creation process. For vendors last paid within 5 years from the date of reactivation request, vendors are reactivated based on an email request from the requesting department. According to the Controller, there was no specific reason for selecting 5 years as a cutoff.

The audit assessed Financial Services' vendor reactivation processes and noted the following:

- There is limited oversight to reactive a vendor who was last paid within the previous 5 years, as an email from the requesting department is the only support required to initiate a vendor reactivation. No additional validation is performed.

- Although the Accounts Payable Supervisor is responsible for reactivating vendors, 48 employees have system functionality to reactive vendors. There does not appear to be any justifiable operational need for this many employees to have this functionality.

- No one reviews or approves the reactivated vendors as the JDE system does not have reporting functionality to flag reactivated vendors for management review.

The absence of appropriate processes and management oversight over vendor reactivations increases the risk of unauthorized and/or inappropriate reactivations, which may increase the risk of error or misappropriation.

It should also be noted that the risk identified in this observation would be significantly reduced by reducing the reliance on LDM procurements, as the need to reactivate a vendor on a going forward basis would likely only occur based on the result of a competitive procurement process.

### Recommendations

We recommend that management:

- Investigate the feasibility of developing a report which flags vendor reactivations and have a member of the Procurement Services Management team review the appropriateness of reactivated vendors.

**VENDOR MASTER FILE AUDIT**

- Determine which employee(s) require the vendor reactivation functionality, based on their job requirements and ensure only those employees have the system user rights to use the functionality.

**Management Action Plan**

Management agrees with these recommendations.

Management will investigate the feasibility of developing a report which flags vendor reactivations and have a member of the Procurement Services Management team review the appropriateness of reactivated vendors.  This will be completed by Q4, 2023.

Management will review access rights with respect to ensure that only appropriately authorized individuals have the ability to reactivate a vendor.  This will be completed by Q4, 2023.

There will be no reactivation for the vendor types that Financial Services has oversight.

### 7. *Transition Medical Note and Safety Footwear Reimbursements from A/P to Payroll*

Per the Full Time Hourly Collective Agreement, section 19.08 states that employees working in areas where safety footwear is required, will provide their own appropriately rated safety footwear, and they will be reimbursed, upon submission of proof of purchase, the cost up to $250 every two calendar years.  Employee medical notes are also a permissible employee expense under the collective agreement. Employees requesting reimbursement must provide appropriate documentation to support the reimbursement.  A/P will set up the employee as a vendor in the vendor master file to process the reimbursement.

Between January 2019 and December 2020, 223 footwear reimbursements were paid to employees for an approximate total of $48,000.  This averages to approximately $215 per reimbursement.  Based on the average A/P invoice processing cost of $90, the estimated cost to make these reimbursements is $20,070 ($90 per invoice processed through A/P x 223).  As this relates to 2 years' worth of footwear reimbursements, making the reimbursement through payroll rather than A/P may generate an estimated annual cost savings of $10,035 per year. The audit did not identify any instances of employees receiving greater than the $250 eligible reimbursement during the audit scope period.

Based on discussions with Financial Planning and Development Finance, they track boot reimbursements in Excel spreadsheets.  Internal Audit reviewed these spreadsheets.  While these spreadsheets provide a detailed history of reimbursement by employee, the manner in which the data is captured would make it difficult to perform more in depth analysis, such as total reimbursements by eligibility period, or percentage of eligible employees who received a reimbursement.  According to management, no cost benefit analysis has been performed for at least ten years to determine whether a bi-annual per diem for footwear reimbursements would be more cost beneficial than the current practice.   After discussing the issue, management conducted a cost benefit analysis which concluded that based on cost and health and safety considerations, the current reimbursement process is preferred over a per-diem system.  Internal Audit concurs with this analysis and decision.

Between January 2019 and December 2020, 444 medical notes were reimbursed to employees for an approximate total of $14,000.  This averages to approximately $32 per reimbursement.  Based on the average A/P invoice processing cost of $90, the estimated cost to make these reimbursements is $39,960 ($90 per invoice processed through A/P x 444). The processing cost is roughly three times the amount of the reimbursement.  As this relates to 2 years' worth of medical note reimbursements, making the reimbursement through payroll rather than A/P may generate an estimated annual cost savings of $19,980 per year.

A significant amount of time and effort is required to setup employees as vendors in the vendor master file for the purpose of issuing reimbursements.  Although other employee expenses have been transitioned from A/P to Payroll, medical note and footwear reimbursements are still being reimbursed by A/P to employees via a cheque.  Industry better practice suggests that streamlining and automating processes leads to decreased processing costs, reduction in human error, and increases in efficiency.

## Recommendations

We recommend that management:

- Reimburse all employee expenses, including medical notes and footwear reimbursements, through Payroll.

- Develop an enhanced boot reimbursement tracking sheet to better facilitate the determination and tracking of how many employees across the City are eligible for the boot reimbursement, how many are actively using the reimbursement, and how much of the eligible reimbursement employees are using every 2 years. This report should also be formatted to present the total boot reimbursements paid to all eligible employees during the collective bargaining period versus the total eligible boot reimbursement.

## Management Action Plan

Management agrees with these recommendations.

Accounts Payable can process medical notes and footwear for payment through Payroll provided they have the proper approved backup in the same manner that expenses are processed. Medical note approval and backup originates in Human Resources and the footwear reimbursement request and backup originates in the department with review by Financial Planning and Development Finance. Processing via payroll can be accommodated by Q3 2022.

Currently the city handles most expense reimbursements through an employee reimbursement process beginning in Accounts Payable and ending in Payroll. In order to have a more sophisticated model including advanced routing, OCIO will need to have a ARR submitted in 2023 to purchase the JDE expense management module which is not currently licensed. Funding for professional services will also be required and implementation timelines require vendor assistance.

In phase 1 of the transition to reimbursement via payroll, medical note and footwear reimbursements were excluded due to the additional manual approval routings required, as they were not typical expense report items. Phase 1 of the transition to reimbursement via payroll did not result in significant cost reductions because Accounts Payable still does the processing and the payment is made through Payroll. The only cost saving in Phase 1 was the cost of processing the cheque. The City would have to purchase the JDE Expense Management Module to remove Accounts Payable from the process entirely. As part of the Finance Modernization program and implementation of the Human Capital Management (HCM) module, management will review the current process for approvals and the approval routing options available.

Management and staff will review and enhance the current boot reimbursement tracking sheet. The recommended data fields will be tracked based on the best information available. This can be completed by Q4 2024 if ARR is approved.