City of Madison Finance Department

Vendor Master File Review

INTERNAL AUDIT REPORT

Audited Entity: City of Madison – Vendor Master File Review (PA-2025-01)

Fieldwork Completion Date: April 29, 2025

Date of Report: June 3, 2025

Table of Contents

Contents

EXECUTIVE SUMMARY

BACKGROUND

The Internal Audit Unit has conducted a comprehensive audit of the City's Vendor Master File Management. The Vendor Master File serves as a critical component of the Accounts Payable (AP) process, containing essential vendor details such as name, address, contact information, and tax identification number (TIN) or Social Security Number (SSN) for individual vendors.

As a key tool in the vendor payment process, it is imperative to maintain the Vendor Master File effectively to prevent unauthorized or improper activity, duplicate payments, and operational inefficiencies. Failure to do so could expose the City to financial risks, data integrity issues, and potential misuse. Additionally, the Vendor Master File is used to track vendors who are required to receive an Internal Revenue Service (IRS) Form 1099 based on the payment type, amount, and business classification.

The Finance Department, Procurement Services, and Accounts Payable (AP) teams are responsible for storing and maintaining vendor records within the City's Enterprise Resource Planning (ERP) system, Munis.

This audit was conducted to assess the adequacy and effectiveness of governance, risk management, and internal controls over the City's Vendor Master File Management.

The audit determined that while the Finance Department and Procurement Services have designed and implemented certain internal controls for vendor file creation and management, there are opportunities for improvement in the areas of file maintenance and ongoing monitoring.

As of January 31, 2025, the Vendor Master File contained 20,880 vendors, classified into one of five status categories, as detailed in the table below.

Vendor Status	Status Description	Total Vendors
Active	Current and established vendors	19,629
Inactive	Vendors moved to inactive status due to lack of activity or going out of business	1,079
One time pay	Vendors used one time to pay multiple recipients	11
Stop (Shutdown)	Vendors that can no longer be used	94
Temporary	Vendors used only for a short time	67
	Total	**20,880**

OBJECTIVES

This engagement aims to assure the City’s management that vendor records are reliable, payment activities are effective, and vendor transactions follow required laws and regulations.

The key objectives of the audit were to evaluate the effectiveness of operations in the following areas:

- Accuracy and completeness of vendor’s data
- Identification of duplicate vendors
- Vendor’s registration and maintenance authorization and approval
- Vendor’s compliance with regulatory requirements

- Identification of inactive vendors
- Vendor Master File – system and access controls
- Vendor payment controls review

SCOPE

The scope of this audit was limited to activities related to the Vendor Master File within the Accounts Payable module of the Munis application. The period reviewed was from January 1, 2020, through December 31, 2024.

To achieve this objective, the audit team conducted a structured evaluation of internal controls and applied targeted audit procedures, including but not limited to the following:

- **Policy and Procedural Review:**
  Assessed the City's Vendor File Management policies, Standard Operating Procedures (SOPs), and internal guidelines to determine their sufficiency in preventing unauthorized vendor activities, duplicate records, and financial risks while ensuring compliance with industry best practices.
- **Stakeholder Interviews and Process Walkthroughs:**
  Conducted detailed interviews and process walkthroughs with key personnel from Procurement, Accounts Payable, and Financial Systems (Munis) teams responsible for maintaining and overseeing the Vendor Master File. These discussions provided insight into existing control mechanisms, risk areas, and potential process inefficiencies.
- **Data Analytics and Risk Assessment:**
  - Performed data analytics testing to identify duplicate vendors, inactive accounts (vendors with no transactions in the last 48 months), and irregularities that could indicate potential fraud or control weaknesses.
  - Assessed vendor payment trends to identify high-risk transactions, potential conflicts of interest, and unusual activity.
- **Sample-Based Compliance and Control Testing:**
  - Reviewed a statistically valid sample of vendor records, including business addresses, Tax Identification Numbers (TINs), W-9 forms, and supporting documentation, to evaluate compliance with vendor onboarding, validation, and verification requirements.
  - Assessed whether vendors requiring IRS Form 1099 reporting were accurately classified and had complete tax documentation on file.
- **System Security and Access Control Review:**
  - Evaluated the adequacy of system security settings and user access controls within the Munis ERP system, ensuring that only authorized personnel have permission to create, modify, or deactivate vendor records.
  - Reviewed segregation of duties to confirm that appropriate checks and balances exist to mitigate fraud risks and unauthorized modifications.

These audit procedures were designed to ensure that the City's Vendor Master File is effectively managed, financial risks are mitigated, and compliance with regulatory requirements and internal policies is maintained.

FINDINGS

1. The data analytics review conducted on the Vendor Master File identified the following key observations:
   - 9,927 out of 19,629 active vendors have had no recorded transactions for over four years (2015–2021), indicating a potential need for vendor status review and cleanup.
   - Six active vendor records were identified as duplicates.
   - A total of 1,079 vendors have been classified as inactive by the Finance team for various reasons, including: vendors going out of business, prolonged periods of inactivity with the City, consolidation of duplicate vendor records, absence of a required Affirmative Action (AA) plan on file, or discrepancies identified during IRS filing reviews.

It is important to note that, despite their inactive status, these vendors can still be used for invoice processing and payments. This presents potential financial and compliance risks, including unauthorized transactions or payments.

- 67 temporary vendor records, created in 2023 and early 2024 for the Final Bill Refund process previously used by the Water Utility Division, have not been deactivated after the discontinuation of the process. This oversight highlights a need for timely vendor record maintenance and deactivation protocols.

These findings underscore the importance of continuous monitoring, periodic vendor file reviews, and enhanced control measures to prevent data integrity issues, unauthorized transactions, and compliance risks.

2. The audit identified instances where employees have been assigned multiple user roles within the same module in Munis, resulting in overlapping and redundant access rights.
   For example, an Accounts Payable (AP) user was found to have both Superuser and AP Admin rights.

   However, since Superuser rights encompass all permissions granted under AP Admin, the AP Admin role becomes redundant and effectively dormant.
   This inefficient role assignment could lead to:
   - Unnecessary complexity in user access management, making it difficult to track and enforce access controls.
   - Potential security and compliance risks, as excessive privileges increase the risk of unauthorized or unintentional system modifications.
   - Reduced effectiveness of role-based access controls (RBAC) by allowing overlapping permissions without clear functional distinctions.

3. The audit revealed that the Procurement team does not have a formalized Standard Operating Procedure (SOP) for this activity, as against what the Procurement team currently have.

   The absence of a comprehensive and structured SOP presents the following risks:
   - Inconsistent execution of processes, leading to potential inefficiencies and errors.
   - Lack of clear guidance for staff, which may result in deviations from the best practices and regulatory requirements.
   - Challenges in training new employees, as standardized procedures are not documented for reference.

4. Additional opportunities for improvement in the City's Federal contracting vendor management were identified, including the need for regular certification and recertification of contracting vendors. Implementing these practices will help ensure compliance with risk assessment protocols and align with industry best practices, ultimately enhancing the accuracy, integrity, and security of the vendor data.

RECOMMENDATIONS

- The Procurement team should collaborate with the Financial Systems Analysts to ensure that the 11,073 non-active vendors identified during this review are properly moved to the "**Stop**" status. This will prevent these vendors from being used in unauthorized payments and transactions.
  Additionally, it is essential that necessary approvals are obtained from Finance Management before making any changes to the vendor's status to maintain compliance with internal controls and approval processes.

- Accounting Services should execute the necessary program in the Accounts Payable (AP) system, (Vendor Merge utility), to merge the existing six (6) duplicate vendor records identified during the review. This process will help eliminate duplicate entries, ensuring that the Vendor Master File remains accurate and efficient.

- In compliance with the best practices, the Procurement and Financial Analyst teams should establish a protocol for an annual review of the Vendor File. This review should involve obtaining approvals from Finance Department management to deactivate vendors with no activity over a specified period.

The review period (e.g., after four years) should be agreed upon with Finance Department management and incorporated into the Vendor File Management SOP.

- As discussed with the Accounting Services Manager, and in alignment with the best practices, the Finance Department management should conduct a comprehensive review of user access rights in the Munis system. This review should focus on identifying and removing dormant or redundant rights from employees who hold multiple rights within the same module. This exercise should be extended across all modules within Munis to ensure that user access is appropriately assigned, eliminating any unnecessary permissions that may compromise the system's security, integrity, and compliance.

- A process should be established to validate the legitimacy of vendor setup or changes in the Vendor Master File before any updates are made. This could be achieved by ensuring that there is supporting documentation from the agency or vendor initiating the set up or changes. During the audit, we observed that no supporting evidence was attached to Munis for numerous vendor information changes.

  Regular access reviews should be implemented to maintain robust control over user permissions and to ensure that access levels align with employees' current job responsibilities. The validation process, in addition to regular reviews will ensure that all vendor changes are properly documented and authorized, reducing the risk of fraudulent or erroneous entries.

- In compliance with the best practices and Enterprise Risk Management protocols, the Procurement team should develop and implement a formal Standard Operating Procedure (SOP) for Vendor File management.

  The SOP should clearly outline the following:
    - The requirement for the use of forms for vendor setup or changes, with signatures from both the requesting agency and the responsible procurement officer to ensure accountability and proper authorization.
    - A checklist of required documentation (specific to each vendor type), which should be thoroughly reviewed and approved for appropriateness before being uploaded into the Munis application. This ensures that only complete and valid vendor records are created in the system.
    - A process should be established for the periodic review and update of Standard Operating Procedures (SOPs) and work instructions to ensure they remain accurate and relevant to the current operating environment.

Regular updates will keep the procedures aligned with the industry's best practices and ensure that operational efficiencies are continuously improved.

- The Internal Audit unit has identified the following process improvement on the federal contracting vendors to ensure regular monitoring and continuous review of the Vendor File management:

A citywide process should be implemented to ensure that vendors continue to meet regulatory and legal requirements. This can be achieved through:

- Vendor certification, where all federal contracting vendors are required to confirm that they meet legal and regulatory requirements before being onboarded into the City's system.

- Annual vendor recertification, where federal contracting vendors are required to confirm that they still meet all legal and regulatory standards.
- Continuous cross-checking of vendor information against government debarment or sanction lists to identify and remove high-risk vendors.
- Enforcing penalties, suspension, or disqualification for vendors that violate regulations, ensuring that only compliant vendors remain active.

Note: See findings and recommendations beginning on page twelve (12) for more detail.

(This Section Was Intentionally Left Blank)

INTRODUCTION

Pursuant to the City of Madison Code of Ordinance Chapter 4.02 (3) and its efforts to ensure financial and operational controls across the City, fostering accountability, and minimizing risks, the Internal Audit has conducted an internal review of the Vendor Master File Management. The audit was conducted in accordance with the Generally Accepted Government Auditing Standards (GAGAS). These standards require the Internal Audit to plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. The control and procedural deficiencies considered to be significant are also disclosed herein. This report does not disclose any perceived weaknesses or findings from external agencies.

BACKGROUND

The Internal Audit unit has conducted an audit of the City's Vendor Master File Management. The Vendor Master File is an essential component of the Accounts Payable process, containing vital information about the vendors the City engages with, such as vendor names, addresses, contact details, tax identification numbers (or SSNs for individual vendors), and other critical data points.

This Vendor Master File is crucial for facilitating vendor payments. Therefore, proper maintenance of this file is essential to prevent unauthorized activities, avoid duplicate payments, and minimize operational inefficiencies. If not maintained adequately, there is a risk of incorrect payment processing and potential misuse of vendor information.

Additionally, the Vendor Master File also tracks vendors required to receive IRS Form 1099 based on specific payment criteria, such as the type of payment, payment amount, and business nature.

Responsibility for Managing the Vendor Master File

The Procurement and Accounts Payable (AP) team of the Finance Department is responsible for storing and maintaining vendor data within the City's financial reporting software, Munis.

More specifically, Procurement Services manages the Vendor Master File, which includes tasks such as:

- Setting up new vendors within the Munis AP Module.
- Updating or changing existing vendor information (e.g., bank account details, contact information) when requested by vendors.

Vendor Setup Process

To set up a new vendor in the Vendor Master File, the following process is followed:

1. **Agency Responsibility**: The relevant employee from each agency collects the required vendor information and documentation and submits it to the Procurement team for further review.
2. **Procurement Review**: The Procurement team reviews the submitted information and documentation to ensure compliance with both the City's policies and applicable regulatory standards. The team also cross-references the data with the City's financial system to ensure there are no duplicate vendor records.
3. **Vendor Creation**: Upon successful review, the Procurement team enters the vendor's details into Munis for record-keeping and payment purposes.

Vendor Invoicing and Payment Protocol

The following procedures are followed for vendor invoicing and payment processing:

- **Invoice Review**: The agency responsible for the service or product verifies and approves the invoice for payment.
- **Accounts Payable Review**: A member of the Finance (AP) team further reviews and approves the invoice for payment.
- **Payment Disbursement**:
  - Check Run: The Accounting Services unit in the Finance Department conducts a weekly check run every Thursday morning, printing physical checks for vendors who require paper payments.
  - ACH Payments: For vendors set up to receive electronic payments, ACH transfers are initiated to facilitate prompt and secure payments.

This audit was conducted to evaluate the adequacy and effectiveness of the governance, risk management, and controls over the City's Vendor Master File. The objective was to assess whether the processes in place effectively mitigate risks, ensure compliance, and promote operational efficiency in managing vendor information.

Internal Audit found that the Finance Department and Procurement Services have designed and implemented several internal controls for the creation and management of vendor files. These controls help in ensuring compliance with the City's policies and regulations. However, there are opportunities for further improvement in the areas of file maintenance and monitoring to enhance overall effectiveness and mitigate potential risks more efficiently.

As of January 31, 2025, the Vendor Master File contained a total of 20,880 vendors. These vendors are classified into one of the five statuses, as shown in the table below, to manage their usage and ensure proper categorization for payment purposes.

Vendor Status	Status Description	Total Vendors
Active	Current and established vendors	19,629
Inactive	Vendors moved to inactive status due to lack of activity or going out of business	1,079
One time pay	Vendors used one time to pay multiple recipients	11
Stop (Shutdown)	Vendors that can no longer be used	94
Temporary	Vendors used only for a short time	67
	Total	**20,880**

SCOPE

The scope of this audit was limited to the Vendor Master File within the Accounts Payable (AP) module of the Munis application. The review focused on assessing the adequacy and effectiveness of controls and processes within this specific system to ensure proper vendor management, payment accuracy, and compliance.

The audit period under review spanned from January 1, 2020, through December 31, 2024, covering a comprehensive five-year window to assess historical data, identify potential trends, and evaluate the impact of past practices on current operations.

AUDIT OBJECTIVES AND METHODOLOGY

The primary objective of this audit engagement was to assure the City's management that vendor records are reliable, that payment activities are effective, and that vendor transactions comply with the required laws and regulations. The key areas of focus for the audit were to assess the effectiveness of operations within the following domains:

- Accuracy and completeness of vendor data.
- Identification and elimination of duplicate vendors.
- Vendor registration, maintenance authorization, and approval processes.
- Vendor compliance with relevant regulatory requirements.
- Identification of inactive vendors and their proper handling.
- Vendor Master File system and access controls.
- Review of vendor payment controls.

To evaluate the effectiveness of controls and assess whether the City's vendor management practices align with the objectives, the following procedures were conducted:

- Review of Vendor File Management policies and Standard Operating Procedures (SOP) to understand the existing protocols for vendor data management.
- Interviews with the Procurement, Accounts Payable (AP), and Financial System (Munis) staff responsible for maintaining and monitoring the Vendor Master File to assess their roles and procedures.
- Data analytics tests were performed to identify and eliminate duplicate vendors and vendors with no transactions for the last 48 months, ensuring the integrity of the vendor list.
- A sample review of vendor data, including addresses, Tax IDs, W-9s, and other supporting documents, to test the effectiveness of controls and verify compliance with City policies and regulatory requirements.
- A review of system and access controls within the Munis application to ensure sufficient security and restricted access to sensitive vendor information.

The Internal Audit conducted interviews with stakeholders and performed reviews of requested documents to determine if:

1. The Procurement Unit has established protocols to ensure that the Vendor Master File records are complete, accurate, and updated in accordance with internal and regulatory requirements. The following procedures were implemented to ensure data quality and compliance:
    a. A full extract of the Vendor Master File was downloaded from Munis and thoroughly reviewed for completeness to ensure all necessary information was captured.
    b. Vendor details were checked to ensure that no critical fields (such as Tax ID, vendor address, or vendor bank details) were left blank. This ensures that essential information is accurately recorded.
    c. A review was conducted to identify and eliminate any ghost vendors—vendors without physical addresses, tax records, or legitimate transactions. These records were flagged and removed to prevent fraudulent entries.
    d. Vendor information was cross-checked against the supporting documents uploaded in the Munis system, ensuring that all details are consistent and substantiated.
    e. Vendor records were reviewed to confirm proper classification. For example, corporate vendors were identified by their Federal Identification Numbers (FIDs), while individual vendors were identified using their Social Security Numbers (SSNs).
    f. The data entry procedures and the internal controls protocols established by the Procurement Unit were reviewed to ensure data integrity was maintained throughout the process. This included verifying that correct validation checks, and security measures are in place.

2. The Procurement Unit has implemented effective controls to prevent, detect, and eliminate duplications of vendor records, thereby reducing the risks of duplicate payments and fraudulent activities. The following steps were taken as part of the vendor record management process:
    a. A data analytics test was performed on the downloaded Vendor Master File using the fuzzy matching method. This method compared vendors' names, tax IDs, and bank account numbers to identify any similar or identical entries that might indicate duplicate records.
    b. Vendors with similar or identical details were flagged for further investigation to determine the cause of the anomalies. This ensured that no vendor was mistakenly duplicated in the system due to data entry errors or other reasons.
    c. Vendor records found to be duplicates were carefully assessed to determine if the duplication occurred due to inadequate controls or was a result of intentional manipulation. This helped identify potential gaps in the process or fraudulent activity that needed to be addressed.
    d. The duplicated vendor records were compared against their respective invoices and payments to verify that no duplicate payments were made during the review period. This ensured that no duplicate records did not lead to the payment of the same invoice multiple times.

3. The Procurement Unit has established strong controls to ensure that all vendors are properly authorized and approved in accordance with the City's policies before their records are created or updated in the Munis system. These steps help to maintain compliance and mitigate the risk of unauthorized changes or fraudulent activities. The following measures were reviewed as part of this process:
    a. Policies and procedures governing the approval of new vendors and updates to vendor records were requested and reviewed to ensure alignment with the City's compliance standards and internal controls. This step ensured that the policies were adequate for preventing unauthorized vendor entries or modifications.
    b. Samples of vendor setups and updates were selected and thoroughly analyzed to confirm that vendor approvals were documented and adhered to the City's policies. This step validated that the process was being followed correctly and consistently across all vendor records.
    c. For the selected samples, we ensured that vendor setups and updates were approved by authorized personnel who had the appropriate authority to make such changes. This ensured that all vendor records had received proper authorization before being processed.
    d. Vendor records were checked for any unauthorized or inactive vendors that may have continued to receive payments. This helped to identify any potential oversight or gaps in the review process that could lead to unauthorized transactions.
    e. An additional check was conducted to identify any vendor records created by unauthorized personnel or entries that lacked appropriate segregation of duties. This ensured that no vendor was added or updated without the necessary approvals and oversight.

4. The Procurement Unit has established protocols to ensure that vendors comply with all necessary tax, legal, and regulatory requirements before being onboarded into the Munis system. These measures are crucial to safeguarding the City from any potential legal, financial, or reputational risks. The following controls were reviewed as part of this process:
    a. Samples were selected from the downloaded Vendor Master File and thoroughly analyzed to verify that tax identification numbers (TINs) were valid. Additionally, for U.S. vendors, the presence of valid W-9 forms was confirmed, and for non-U.S. vendors, the necessary W-8 forms were checked. This ensured compliance with tax reporting requirements and proper documentation for each vendor.
    b. The documentation for each vendor was reviewed to confirm that they were in compliance with the required legal and regulatory documents based on their specific classification. For instance, this included ensuring that corporate vendors had the necessary tax forms, and individual vendors had the correct identification documents to meet applicable tax laws.

c. The Procurement Unit’s protocols were reviewed to verify that vendor information was regularly cross-checked against government debarment lists, such as those provided by SAM.gov and OFAC (Office of Foreign Assets Control). This ensures that the City does not engage vendors who have been sanctioned or debarred from doing business with government entities.

d. Samples of vendor records were reviewed to ensure that all vendors adhered to procurement policies and documentation requirements. This review ensured that vendor information was properly documented and that all required forms and compliance checks were completed before vendor set up in Munis.

5. The Procurement Unit has implemented controls to effectively identify and review inactive or high-risk vendors that could pose financial risks or be used for fraudulent activities. These measures help the City mitigate the potential for unauthorized transactions and reduce exposure to fraud. The following steps were taken to evaluate these controls:
   a. Data analytics was performed on the downloaded Vendor Master File to identify vendors that had no activities or transactions over the past 48 months. This analysis helped highlight vendors that may no longer be actively engaged in business with the City and could be at risk of being misused for fraudulent transactions.
   b. The Vendor Master File was reviewed to verify whether the Procurement team has a clear protocol in place for the periodic review and deactivation of inactive vendors. Ensuring that inactive vendors are regularly reviewed and properly deactivated minimizes the risk of unauthorized payments being processed through obsolete vendor accounts.
   c. Samples from the Vendor Master File were selected and analyzed to identify vendors with excessive transactions compared to industry norms. This review helps identify any vendors with unusual activity patterns that might indicate fraudulent behavior or improper use of the vendor file.
   d. For vendors with large or unusual transaction volumes, samples were reviewed to ensure that these vendors were periodically reviewed for compliance with relevant policies and regulations. This review ensures that high-transaction vendors are continuously monitored for any irregularities or signs of misuse.

6. The Procurement Unit has established protocols to ensure that access to the Vendor Master File is restricted and appropriately controlled to prevent unauthorized modifications and protect the integrity of the file. These protocols are crucial to maintaining security and compliance with relevant regulations. The following steps were taken to evaluate these controls:
   a. A list of employees with access to the Vendor Master File over the past 24 months was downloaded and analyzed. This allowed for a comprehensive assessment of who has access to the file and whether such access is appropriate based on job responsibilities.
   b. User access was reviewed against each employee's job description to ensure that access is limited to job requirements. Additionally, it was verified that access was appropriately approved by relevant authorities to ensure there are no instances of unauthorized access or excessive privileges granted to employees.
   c. The user access logs were reviewed to identify any unauthorized changes made to the vendor records. This review helps detect any suspicious activity or breaches in protocol that could indicate potential issues with data integrity or unauthorized access.
   d. The access protocols were evaluated to ensure proper segregation of duties for roles involved in vendor file maintenance. This review ensures that no single individual has full control over all aspects of the vendor file creation, updating, and approval processes, thereby reducing the risk of fraud and errors.
   e. System controls were reviewed to ensure that adequate provisions are in place to prevent unauthorized modifications to vendor records. This includes technical safeguards, such as access

restrictions, change logging, and approval workflows, that protect the integrity of the Vendor Master File.

The following section contains a detailed listing of each audit finding, applicable internal audit recommendations, and audit observations.

FINDINGS AND RECOMMENDATIONS

Reference 1: Results of the Data Analytics on the Vendor Master File.

Finding

We performed comprehensive data analytics on the Vendor Master File to identify vendors with no activities for over 48 months, duplicate vendors, and any high-risk vendors that may require additional scrutiny. The findings are as follows:

- 9,927 of the 19,629 active vendors have had no transactions for a period of more than 4 years (2015 – 2021). These vendors represent potential risks, as their continued presence in the system could lead to unauthorized payments or inefficient processing.
- 6 active vendors were identified as duplicate records. Duplicate vendor entries can result in the risk of duplicate payments or fraud, highlighting the need for a systematic process to identify and eliminate such instances.
- A total of 1,079 vendors are currently marked as inactive in the system. Vendors may be moved to an inactive status for several reasons, including going out of business, prolonged inactivity with the City, consolidation of duplicate vendor records, lack of an Affirmative Action (AA) plan on file, or IRS filing discrepancies.

  However, it is important to note that vendors with an inactive status can still be invoiced or paid, which presents a potential risk of unauthorized or inappropriate transactions. This gap in control may undermine the effectiveness of the vendor management process and expose the City to financial risks.
- 67 temporary vendors, created in 2023 and early 2024 for the Final Bill Refund process formerly used by the Water Utility Division, have not been deactivated after the Division ceased using the process. These vendors represent potential risks of misuse or incorrect payments due to their continued active status in the system.

In addition to the findings above, we observed that the Procurement team currently does not have a protocol in place for annual reviews of vendor records to identify inactive or dormant vendors. Reviews are done on an as-needed basis and not as part of the standard Procurement unit policy. Implementing an annual review process would enhance vendor record accuracy and help ensure the continued validity of vendor relationships.

Criteria

- Inactive vendors should be regularly reviewed and monitored to confirm that they are still operational business entities and are willing to continue doing business with the City. If a vendor no longer exists or is unwilling to continue business with the City, their records should be deactivated in the Vendor Master File to prevent unauthorized transactions and ensure data accuracy.

Recommendation

- The Procurement team should collaborate with the Financial Systems Analysts to ensure that the 11,073 non-active vendors identified during this review are properly moved to the "**Stop**" status. This will prevent these vendors from being used in unauthorized payments and transactions.

  Additionally, it is essential that necessary approvals are obtained from Finance Management before making any changes to the vendor's status to maintain compliance with internal controls and approval processes.

- Accounting Services should execute the necessary program in the Accounts Payable (AP) system, (Vendor Merge utility), to merge the existing six (6) duplicate vendor records identified during the review. This process will help eliminate duplicate entries, ensuring that the Vendor Master File remains accurate and efficient.

- In compliance with the best practices, the Procurement and Financial Analyst teams should establish a protocol for an annual review of the Vendor File. This review should involve obtaining approvals from Finance Department management to deactivate vendors with no activity over a specified period.

The review period (e.g., after four years) should be agreed upon with Finance Department management and incorporated into the Vendor File Management SOP.

Management Response
Accounting Services staff will plan to draft a procedural policy for MUNIS vendor maintenance going forward. This will identify the varying status types available within the vendor master file; how they are used city-wide; procedures for obtaining approvals to migrate active vendors to other status types (i.e. active or inactive to a stop status based upon inactivity); and to establish the frequency by which the Vendor Master File will be reviewed. Staff will submit and implement the new procedural policy by 6/30/2025.

- Here is an updated summary of our current vendor records and their corresponding status since receiving this report:

Status	Count of Vendors
Active	12778
One Time Pay	11
Stop	8395
Grand Total	**21184**

- 8,308 vendor records were moved to Stop status on 4/11/2025.
    - 7,162 with no activity since 12/31/2019 (vendor inactivity may be skewed for fiscal years 2020 and 2021 given the COVID-19 pandemic). Finance Department Purchasing staff used an inactive date as of 12/31/2019.
        - An additional 2,764 vendors would move to Stop status if purchasing staff used a 12/31/2021 date. These remain currently inactive until further review at the end of fiscal year 2025.
    - 1,079 that were in Inactive status
    - 67 that were in Temporary status

Additionally, six duplicate records were merged to eliminate the redundant vendor records identified during this review.

Implementation Date
June 30, 2025

Reference 2: Employees with multiple user's right within the same Module.

Finding

Our review of employee access to the Vendor Master File and associated records revealed that several employees have multiple user rights within the same modules in Munis, leading to one right overriding the other. For example, an Accounts Payable (AP) user may have both Superuser and AP Admin rights. In such cases, the Superuser rights take precedence, rendering the AP Admin rights inactive.

Note: Since the scope of our review was limited to vendor records within the AP Module, Internal Audit was unable to conduct similar tests across other modules.

This inefficient role assignment could lead to an increased risk of an employee being given an inappropriate role in error. An employee with an inappropriate role applied to their Munis profile could lead to:

- Unauthorized or improper access to sensitive data.
- Unnecessary complexity in user access management, making it difficult to track and enforce access controls.
- Potential security and compliance risks, as excessive privileges increase the risk of unauthorized or unintentional system modifications.
- Reduced effectiveness of role-based access controls (RBAC) by allowing overlapping permissions without clear functional distinctions.

Further inquiries revealed that there have been instances in the past where users' rights were not updated following a change in their job function, leaving dormant rights active and not removed.

Criteria

- Employees' access rights should be aligned with their current job functions. When an employee's role or responsibilities change, access rights associated with their previous roles should be promptly deactivated or removed to prevent unauthorized access to sensitive information.

Recommendation

- As discussed with the Accounting Services Manager, and in alignment with the best practices, the Finance Department management should conduct a comprehensive review of user access rights in the Munis system. This review should focus on identifying and removing dormant or redundant rights from employees who hold multiple rights within the same module. This exercise should be extended across all modules within Munis to ensure that user access is appropriately assigned, eliminating any unnecessary permissions that may compromise the system's security, integrity, and compliance.

- Regular access reviews should be implemented to maintain robust control over user permissions and to ensure that access levels align with employees' current job responsibilities.

Management Response

Currently, there are approximately 830 users within MUNIS with two Financial Systems Analyst administering access. Given internal discussions, Accounting Services staff recommend creating a 5-year rolling schedule in which the Financial Systems Analysts annually review 20-25% of the system's users and their respective roles/permissions. They will formally request City supervisory staff complete a questionnaire, and/or form confirming current departmental users and their roles/permissions.

Accounting Services staff do not align other department's employees' job responsibilities to MUNIS access, but we can work to establish a more formal review of user roles and permissions annually.

Implementation Date

June 30, 2025

(This Section Was Intentionally Left Blank)

Reference 3: Documentation of the Vendor Master File Standard Operating Procedure (SOP).

Finding

Our review of the vendor file management process revealed that the Procurement unit does not have a formally documented Standard Operating Procedure (SOP). Although a step-by-step document outlining the activities involved in setting up a vendor in Munis was provided to the Internal Audit, this document does not constitute a formal SOP.

Additionally, the document provided to the Internal Audit does not include other related activities associated with the maintenance of vendor records such as a checklist or reference guide outlining the required documentation that prospective vendors must submit before being set up in the City's financial system (Munis). It also does not provide evidence that vendor-initiated requests for updates or changes to their records are consistently reviewed and approved by designated staff within the Procurement unit.

As part of best practice, the Standard Operating Procedure (SOP) should not only be formally documented, reviewed, and approved by Finance Department management as the official guide for vendor record management, but it should also be periodically reviewed. This ensures that it accurately reflects current operational processes and aligns with internal control expectations and evolving business needs.

Criteria

- The Institute of Internal Auditors (IIA) (**Practice Advisory Standard 2130.A1-1**) and the U.S. Government Accountability Office (GAO) through Generally Accepted Government Auditing Standards (GAGAS) emphasize the importance of internal controls, policies, and procedures (including Standard Operating Procedures, or SOPs), and their periodic review, and approval by the by the unit or department management as the official operational manual. This ensures consistency, accountability, and clarity in the execution of processes and helps mitigate risks associated with errors or omissions.

- The use of standardized documentation, such as checklists, is essential to ensure consistency and compliance across vendor record management processes. Checklists provide a clear and uniform approach to vendor onboarding, updates, and reviews, promoting operational efficiency and minimizing the risk of errors or omissions.

- Implementing a regular review process would help maintain the SOP’s relevance and effectiveness.

Recommendation

- In compliance with the IIA and GAGAS Standards and Enterprise Risk Management protocols, the Procurement team should develop a formal Standard Operating Procedure (SOP) for Vendor File management. The SOP should mandate the use of forms for vendor setup or changes, with sign-off from both the requesting agency and the responsible procurement officer. Additionally, a checklist of required documentation (specific to each vendor type) should be reviewed, approved for appropriateness, and uploaded into Munis before any vendor is set up in the system. This will help ensure proper documentation, consistency, and compliance with the City's policies.

- A process should be established to validate the legitimacy of vendor setup or changes in the Vendor Master File before any updates are made. This could be achieved by ensuring that there is supporting documentation from the agency or vendor initiating the set up or changes. During the audit, we observed that no supporting evidence was attached to Munis for numerous vendor information changes.

This validation process will ensure that all vendor changes are properly documented and authorized, reducing the risk of fraudulent or erroneous entries.

- A process should be established for the periodic review and update of Standard Operating Procedures (SOPs) and work instructions to ensure they remain accurate and relevant to the current operating environment.

Regular updates will keep the procedures aligned with the industry’s best practices and ensure that operational efficiencies are continuously improved.

Management Response

Currently, we complete a detailed checklist for updating the vendor master file such as address, contacts, and/or banking information. Accounting Services staff will create an internal control matrix and will review the document annually and/or more frequently for changes. Baker Tilly also reviews all city prepared matrices annually as part of their internal control testing procedures. We will add this one by 9/30/2025.

Additionally, a specific form or checklist for vendor master file set-up, validation, and other updates will be completed, approved, and attached within MUNIS.

Implementation Date
September 30, 2025

(This Section Was Intentionally Left Blank)

CONCLUSION

The Finance Department has implemented various controls to manage the City's vendor records. However, the Internal Audit has identified opportunities to enhance the effectiveness and efficiency of the Vendor Master File management. These improvements include conducting regular reviews of inactive and duplicate vendors, addressing complexities in user access management due to employees holding multiple user rights, formally documenting Standard Operating Procedures (SOPs) for vendor record maintenance, instituting an annual review process for vendor records, validating vendor setups and record updates, and ensuring ongoing compliance with legal and regulatory requirements.

As part of its future engagements, the Internal Audit Unit will conduct a comprehensive review of the City's contracting processes. This review will encompass key elements such as the vendor certification and re-certification procedures, contract approval workflows, and compliance with applicable policies and regulations. The objective of this audit is to evaluate both the design and operating effectiveness of the City's internal controls related to vendor management and contracting activities. The findings will help identify potential risks, strengthen oversight, and support process improvements to ensure transparency, accountability, and efficiency in the City's procurement practices.

The City of Madison Finance Department, Internal Audit Unit, extends its appreciation to the Procurement Unit staff, Financial Systems Analysts, and all individuals who contributed to this audit. Their professionalism, cooperation, and support were instrumental in the successful completion of this review.

(This Section Was Intentionally Left Blank)

ACKNOWLEDGEMENT

The Vendor Master File Review

Compiled by | Kolawole Akintola, Internal Audit and Grant Manager

Reviewed by | David Schmiedicke, Finance Director

Signing below certifies that you have received, read, and acknowledge the audit report prepared above.

David Schmiedicke 6/3/2025

David Schmiedicke, Director Finance Date

Patricia A. McDermott 6/3/2025

Patricia A. McDermott, CPA, Accounting Services Manager Date