INTERNAL AUDIT REPORT

Department of Finance & Administration - Financial Services and Supply Chain Divisions

Vendor Master File, Electronic Funds Transfer and Wire Transfer Audit

Assignment # 19-02

INTERNAL AUDIT REPORT

Department of Finance & Administration - Financial Services and Supply Chain Divisions

Vendor Master File, Electronic Funds Transfer and Wire Transfer Audit

Assignment # 19-02

Sean McGrath, CPA, CA,
CFE
Senior Internal Auditor
February 19, 2020

Sean P. Janes, CPA, CMA,
CIA, CFE
City Internal Auditor
February 19, 2020

ST. JOHN'S

TABLE OF CONTENTS

To: Chair & Council Members, Audit Committee

Area Responsible: Deputy City Manager – Finance & Administration
Manager – Financial Services
Manager – Supply Chain

Copy to: City Manager

INTRODUCTION

OBJECTIVES

The objectives of this review were to assess whether key controls over the vendor master file, electronic funds transfer, and wire transfer processes were adequately designed and operating as intended.

METHODOLOGY AND SCOPE

The audit focused on controls surrounding the accuracy, completeness, authorization, and validity of vendor master file ("VMF"), electronic funds transfer ("EFT") and wire transfer details and payments. The audit also assessed whether controls were in place that deter and detect fraud.

To meet the audit objective, research was conducted on best practices regarding internal controls for the VMF, EFT and wire transfer processes. In addition, audit procedures were performed including interviews with management and staff, system walk-throughs, analysis of supporting documentation and substantive testing of VMF, EFT and wire details. Additionally, numerous fraud analytical procedures were performed on VMF and EFT details.

All vendor types were included in the scope of the audit. This included external vendors setup for the purchasing of goods and services, external vendors setup for one-time payments such as tax refunds and legal settlements, and City of St. John's employee vendors who receive reimbursement for non-salary expenditures. All vendors and EFT transactions as of November 28, 2019 were included for purposes of performing analytical procedures (e.g., determining the number of inactive vendors, duplicate vendors, total vendors, etc.). However, in the case of substantive testing (e.g., examination of EFT setup forms), samples were chosen from the 2019 and 2018 years only.

The VMF interacts with other processes such as requisitioning, purchase order issuance, receiving, keying of invoices and batch payment. These processes were predominantly scoped out of the audit and were only considered from a segregation of duties perspective.

BACKGROUND

Vendor Master File (VMF)

The VMF is an essential component of both the accounts payable and procurement processes as it contains vital information about vendors the City does business with. The VMF includes information such as vendors' names, addresses, telephone numbers and banking information. The data in the VMF is used to process payments to City vendors and thus it is imperative that such data is accurate and complete. Furthermore, strong internal controls are required in an effort to mitigate the risks of fraud and erroneous payment.

The City's VMF contains purchasing vendors, employee vendors and one-time vendors. Purchasing vendors are traditional suppliers that provide goods and services to the City, while employee vendors are City employees who are entitled to reimbursement for costs such as training, membership fees, travel, etc. One-time vendors are vendors that are entitled to a payment from the City for things such as legal and insurance settlements, court fees and tax refunds. The City's Supply Chain Division is responsible for adding purchasing vendors to the VMF, while the Financial Services Division is tasked with adding employee and one-time vendors. Both divisions are responsible for the maintenance and administration of their applicable vendors.

The City uses Microsoft Dynamics GP ("GP") to capture and store vendor information. As of November 2019, the City's VMF contained over 16,000 vendors. A breakdown of vendors by class and status can be found in Table 1.0.

Table 1.0 – City of St. John's Vendors

Vendor Class	**Number of Vendors**	**% of Total Vendors**	**Vendor Status by Class**		
			Active	*Inactive*	*Temporary*
Canadian	14600	90%	3753	131	10716
Employee	1276	8%	770	457	49
US	344	2%	260	1	83
Other	7	0%	3	0	4
Totals	**16227**	**100%**	**4786**	**589**	**10852**

Electronic Funds Transfer (EFT)

City vendors have an option to be paid via EFT instead of receiving a cheque. Financial Services is responsible for collecting EFT information from vendors and ensuring the accuracy and completeness of EFT details and payments. EFT banking information is entered in the VMF along with other vendor information.

Financial Services uses two EFT forms to gather banking details from vendors – an employee EFT form and a vendor EFT form. Access to EFT details is restricted and can only be accessed by one of the Financial Accountant II's ("Accountant") and the Financial Services Manager. The Accountant is responsible for entering the EFT details into the VMF, while the Financial Services Manager is responsible for reviewing the details and supporting EFT form.

The City utilizes the Royal Bank of Canada’s online banking system (“RBC Express”) to facilitate EFT payments. To make an EFT payment, an Accountant in Financial Services generates an EFT payment file from GP. This payment file includes a batch of EFT payments that are to be paid on the next upcoming pay date. When the file is generated in GP, it is automatically saved on the City’s finance drive as a text file. The text file format is necessary as this is the format accepted by RBC Express for upload. An Accountant in Financial Services performs the upload to RBC Express.

Wire Transfer Payments

Wire transfers are completed online through RBC Express. The majority of wire transfers at the City are scheduled recurring payments in relation to bonds, sinking funds and grants. The Manager of Financial Services, Manager of Budget and Treasury and Deputy City Manager of Finance and Administration are all administrators on the Wire Payments Service within RBC Express. Most wire transfers are initiated by the Financial Accountant III in Financial Services and each transfer requires two approvers in order to release the payment. Each administrator is an approver for wire transfers.

While the volume of wire transfers is far less than the volume of EFT vendor payments, millions of dollars can be transferred in a single wire transaction. Therefore, it is essential that strong internal controls are implemented to protect against unauthorized and fraudulent usage.

CONCLUSION

The audit determined that the City of St. John’s had numerous key controls in place that supported strong VMF, EFT and wire transfer processes. However, the design of some of these controls can be further improved. As such, opportunities exist to strengthen controls and improve the accuracy, validity, and completeness of VMF, EFT and wire transfer data.

Furthermore, the audit identified areas where additional controls should be implemented. Many of these new controls are preventive controls that are designed to stop errors or fraud from occurring. Although many detective controls were in place for the VMF, EFT and wire transfer processes, the implementation of these new preventive controls would strengthen the overall control environment.

EXECUTIVE SUMMARY

Internal Audit's review of the vendor master file, electronic funds transfer, and wire transfer processes was undertaken in accordance with the approved three-year audit plan. The audit focused on whether adequate controls were in place and operating effectively in relation to these processes.

Audit testing and procedures utilized during the review identified several positive outcomes. Foremost, Internal Audit performed numerous audit procedures designed to detect fraudulent changes to vendor master file and electronic funds transfer payment information. These audit procedures, which included both analytical and more rigorous substantive testing, did not detect any instances of fraudulent activity.

Additionally, the City had some controls already in place that supported strong vendor master file and electronic funds transfer processes. Such controls included the use of standardized forms, system access controls, management review, validation procedures, audit reports and documented procedure outlining certain tasks.

However, the audit identified areas for improvement regarding several existing controls, as well as opportunities for the development and implementation of new controls. Many of these improvements centered on strengthening segregation of duties, developing, and implementing vendor procedures to help ensure accurate, complete, and valid vendor details, developing and implementing a management monitoring process and developing policy to govern each process.

The observations and recommendations outlined in this report will assist the City in its continued effort to maintain and safeguard the vendor master file, electronic funds transfer and wire transfer processes effectively going forward.

DETAILED ANALYSIS

Section 1 – Vendor Master File (VMF)

Issue 1.1 - Authorization and Review

Vendor authorization and review means that a request for vendor setup or changes to vendor details is reviewed and signed off by a responsible employee prior to taking effect in the VMF system. Inadequate vendor approval and review increases the risk of inaccurate and/or incomplete information being captured in the VMF. Additionally, a lack of review increases the likelihood of fraud as fraudulent or fictitious vendors may not be detected.

The Supply Chain Division utilizes a vendor change form to document requests for new vendors or changes to current vendor information. Vendors complete this form and provide it to the Supply Chain Admin Clerk for entry into the VMF. The Clerk is responsible for entering/amending vendor details in the VMF, signing off on the form, and providing it to the Supply Chain Manager for review.

However, the audit determined that any changes to vendor information take effect immediately in the VMF. Therefore, vendor details were being changed prior to management’s authorization and review. Additionally, Supply Chain management indicated that the actual vendor information entered in the VMF is not reviewed in detail.

Financial Services does not utilize a vendor change form to add employee vendors and one-time vendors to the VMF. Instead, relevant details are taken from cheque requisition forms and entered into the VMF by the Accounting Clerk. Financial Services management indicated that the cheque requisition form is reviewed and signed off on, but the actual vendor details entered into the VMF are not reviewed. Consequently, Financial Services was also not adequately authorizing and reviewing vendor details in the VMF.

Microsoft Dynamics GP, the system used to capture and store vendor information, contains various “workflows” that allow system administrators to define an approval process when records are changed. Internal Audit confirmed with the City’s Corporate Information Services Division that this workflow is available for use but not currently being utilized. If implemented, approvers would be notified when vendor information is added/changed, and these changes would require approval before taking effect in the system. This feature would strengthen internal controls regarding vendor approval and authorization.

Recommendation 1.1

Management should implement the vendor approval workflow feature in Microsoft Dynamics GP to ensure all vendor detail changes are adequately authorized and reviewed. If this is not possible, all requests for vendor set up or changes to a vendor’s information should still be authorized and reviewed by a responsible employee prior to taking effect in the VMF.

Management Response and Action Plan 1.1

Management worked with Information Services to test the approval workflow feature in Microsoft GP. As the GP application is hosted in a Citrix environment and the required email client is hosted on local computers, there is no practical implementation method for this approach. Given this, a process will be developed to ensure vendor details are validated prior to taking effect in the VMF. This will be part of the procedures document which will be created.

Conclusion 1.1

Management has determined that the specific recommendation is not feasible but has committed to developing an alternate process which would achieve the same result.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: December 2021

Information Only: DCM, Finance and Administration

Issue 1.2 - Vendor Validation

Vendor validation is the process of confirming the legitimate existence of vendors through an external source prior to adding them to or making changes to the VMF. This validation process adds reasonable assurance to the legitimacy of new vendors and vendor changes thereby reducing the risk of VMF fraud. Furthermore, vendor validation ensures high data quality and consistency as it also confirms the accuracy and completeness of information.

The audit determined that only banking information was being validated at the City, other details, such as mailing and contact information, were not being validated. This absence of validation is of particular significance to purchasing vendors as they can receive large, recurring payments that are attractive to fraudsters. Furthermore, many vendors still receive payment by cheque and hence a fraudulent vendor change form requesting a change in address could potentially redirect payment to a fraudster.

Most VMF fraud schemes involve inserting a fraudulent vendor in the VMF and thus it is essential that all vendor details are validated prior to being added to the VMF. Additionally, to ensure an appropriate segregation of duties, the person tasked with validating the information should not be able to edit vendor details in the Microsoft Dynamics GP system. This control will mitigate the risk of a person falsely validating a vendor and making fraudulent changes to the VMF.

Recommendation 1.2

i) All vendor information should be validated for legitimacy prior to setting up or amending a vendor.

ii) Vendor information should be validated by someone who cannot edit VMF information in Microsoft GP.

Management Response and Action Plan 1.2

Response from Supply Chain Division

i) Agree – A validation process will be implemented prior to adding or changing vendor information.

ii) Agree – A validation process will be implemented prior to adding or changing vendor information.

Management will validate information by checking websites and/or contacting the company directly. Once approved the authorized vendor form will be forwarded to the Supply Chain Administration Clerk for data entry. The process will begin once the new vendor form is complete.

Response from Financial Services Division

i) Financial Services add/edit vendor master file for non-procurement type vendors. The validation is done prior to sending the request for payment to Finance for processing including, but not limited to, tax refunds, program or security refunds, community grants, employee allowances/reimbursements, fees and expenses relating to legal claims.

ii) Access to the vendor master file has been limited to the greatest extent possible recognizing operational limitations. As a detective control audit trails will be reviewed monthly to ensure only authorized staff are adding/editing records in the vendor master file.

Conclusion 1.2

Both recommendations 1.2(i) and 1.2(ii) will be implemented as stated above for vendors added by Supply Chain Division.

Financial Services management stated that vendors they add to the VMF have already been validated prior to coming to Financial Services for processing. However, Internal

Audit has not confirmed this assertion but will address it during follow-up work. Management also indicated an audit report will be reviewed monthly for unauthorized adding/editing of vendor records which may be indicative of fraudulent activity.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: January 2021

Information Only: DCM, Finance and Administration

Issue 1.3 - Segregation of Duties

Segregation of duties separates roles and responsibilities to ensure that an individual cannot process a transaction from initiation through to payment without the involvement of others, thereby reducing the risk of fraud or error to an acceptable level. As part of the audit Internal Audit reviewed the segregation of duties for the VMF. See Table 2.0 for results.

Table 2.0

Vendor Master File Segregation of Duties – Incompatible Duties

Duty #1	**Duty #2**	**Appropriately segregated?**
Create and maintain a vendor in the VMF	Key an invoice	Yes
Create and maintain a vendor in the VMF	Approve an invoice for payment	No
Create and maintain a vendor in the VMF	Release/approve a purchase order	No
Create and maintain a vendor in the VMF	Create a purchase requisition	No
Create and maintain a vendor in the VMF	Approve changes to the VMF	No

The audit identified several duties that are incompatible in relation to the VMF:

- Four individuals were found to have the ability to edit a vendor and enter a purchase order in the Microsoft Dynamics GP system.

- One individual could edit a vendor and also had a security admin role in the Workplace system used for purchasing, thereby having the ability to make themselves an approver on purchase orders.

- One person was identified as being able to edit a vendor and approve invoices for payment.

- Given that no one was reviewing changes in the VMF, the seven individuals who could edit the VMF were effectively approving changes themselves.

The above noted duties are incompatible from a segregation of duties perspective. However, it should be noted that management approval is generally required at the City to perform most of the above duties (i.e., approve an invoice, release a purchase order, create a purchase requisition). This is a mitigating control which reduces, but does not fully eliminate, the risk related to these segregation of duties issues.

Recommendation 1.3

Management should ensure that the duty of editing VMF details is appropriately segregated from the duties of issuing purchase orders, approving invoices for payment, creating requisitions and approving VMF changes.

Management Response and Action Plan 1.3

<u>Response from Supply Chain Division</u>

The ability to edit a vendor has been removed from 3 of the 4 individuals. Due to operational requirements, it will not be possible to remove the ability to create a PO and edit a vendor from the Supply Chain Administration Clerk as these are key areas of responsibility for this position.

Response from Financial Services Division

Access to the vendor master file has been limited to the greatest extent possible recognizing operational limitations. Detective measures are in place to ensure staff are only making changes to vendor master file as authorized. Further changes will be considered to improve controls around segregation of duties.

Conclusion 1.3

Management indicated the recommendation has been implemented to the greatest extent possible given operational requirements. As such, the duties have not been completely segregated. However, management indicated there are detective controls in place which would help detect fraudulent activity if it were to occur. Additionally, management will attempt to develop additional procedures as operating policies are developed.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: Complete

Information Only: DCM, Finance and Administration

Issue 1.4 - Vendor Master File Policy

Best practice suggests that VMF policies should be robust enough to provide direction to employees on all aspects of the VMF, including how VMF information is captured and maintained. Additionally, strong VMF policies also address other topics including authorization and review, vendor workflow, vendor validation, key segregation of duties, vendor procedures and monitoring.

The audit indicated that there was no formal VMF policy at the City. The absence of such policy can lead to a lack of accountability as VMF roles and responsibilities may not be formally defined. Additionally, an absence of policy increases the risk that critical activities may not be performed, thereby reducing the integrity of the VMF.

The involvement of both Financial Services and Supply Chain in the VMF heightens the need for adequate policy. Management from both Financial Services and Supply Chain indicated they were sometimes unsure of their responsibilities in relation to the VMF and were not always aware of the involvement of the other division. Developing a policy to establish governance and ownership of the VMF would help clarify roles, expectations, and responsibilities.

Recommendation 1.4

Management should develop and implement a formal VMF policy that outlines the roles and responsibilities of those involved in the VMF and addresses key controls such as vendor authorization and review, vendor workflow, vendor validation, segregation of duties and vendor procedures.

Management Response and Action Plan 1.4

Operating procedures will be developed during 2021.

Conclusion 1.4

Management intends to resolve this issue through the development of operating procedures. Management also indicated during subsequent discussions that they will develop a formal policy as time and resources permit.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: December 2021

Information Only: DCM, Finance and Administration

Issue 1.5 - Accuracy and Completeness of VMF Details

It is essential that VMF details are accurate and complete to facilitate efficient and effective accounts payable and procurement processes. As part of testing Internal Audit reviewed the integrity of the VMF as of November 28, 2019. This included performing various analytical tests on the population of 16,227 vendors to test for accuracy and completeness. Substantive testing was also performed as vendor information was verified against corresponding vendor change forms and cheque requisitions. The following observations were made:

- There were issues in relation to the completeness of vendor data, especially regarding direct contact information. 11,780 (73%) of vendors did not have a contact person listed while 11,960 (74%) of vendors were missing a phone number. The omission of direct contact data impedes the validation process and can cause inefficiencies in the payment process.

- Approximately 435 vendors (3%) were identified as potentially being duplicates, which increases the risk of making a duplicate payment to a vendor and may also increase the risk of fraud.

- 2094 vendors (13%) had a PO Box listed as their primary address. While PO Box addresses may be justified for valid business reasons, every effort should be made to obtain a physical address to mitigate the risk of making payments to a fictitious vendor.

- There were issues in relation to the activity level of vendors and whether they should be archived. For example, 9,152 vendors (56%) had not received payment since at least 2016 and 1,286 (8%) had never been paid. Furthermore, of the 4,786 active vendors, there were 1,095 vendors that never received a payment but were still setup as active.

- Audit testing also identified 51 employees who terminated employment with the City between January 1, 2017 and November 21, 2019 but were still listed active in the VMF.

- Of the 1,450 “temporary” vendors paid in 2019, almost half of those were setup between 2010 and 2017. Per the Microsoft Dynamics GP System Guide, a temporary vendor is “a person or company you have a short-term relationship with and are keeping minimal information for.” Given this, it is likely many of the City’s temporary vendors were classified inaccurately.

- Other less frequent inaccuracies (between 0.5% and 1% of the population) included vendors with incorrect classes (e.g., an employee vendor setup as a Canadian purchasing vendor) and vendors with missing addresses.

Inaccurate and incomplete vendor master file data can have numerous ramifications on the accounts payable and procurement processes including missing payment discounts and contract incentives, providing management with inaccurate and/or incomplete information for decision making purposes, increasing fraud opportunities, and increasing the risk of duplicate payments. Therefore, it is imperative that vendor master file data is as complete and accurate as possible.

Recommendation 1.5

Management should initiate a project to clean up the VMF. Clean up should include removing duplicate vendors, archiving inactive vendors and former employees, addressing incomplete/inaccurate fields, and applying a standard naming convention.

Management Response and Action Plan 1.5

A listing of all vendors with a status of active which had no payment activity since 2018/12/31 and prior was created. 9910 vendors on this list have been assigned a status of inactive. Currently there are 2689 active vendors, and the list of active vendors is expected to decrease as further reviews are done.

The Manager of Supply Chain and Manager of Financial Services are reviewing the remaining active vendors to identify possible duplicates for action.

Efforts are ongoing to update the remaining active corporate vendors missing telephone numbers. Once the aforementioned process is complete additional work will take place to clean up the VMF as described in this recommendation.

Conclusion 1.5

Management indicated that the process to implement the recommendation has begun and that the process will take some time to complete. Updates will be provided through follow-up work.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: On-going

Information Only: DCM, Finance and Administration

Issue 1.6 - Vendor Master File Procedures

An underlying cause of the accuracy and completeness issues identified in Issue 1.5 was the lack of adequate VMF related procedures. While documentation did exist regarding how to add a vendor to the VMF, procedures such as naming conventions, vendor deactivation and scheduled maintenance had not been developed and implemented at the City.

The overall administration of the VMF could be improved if such procedures are developed and formally documented. Further details around these procedures are outlined below.

i) Naming Convention and Vendor Setup

Naming conventions are a set of rules that help ensure accuracy and completeness by mandating what vendor details need to be captured in the VMF and how they should be captured.

Audit testing identified consistency issues in vendor names regarding the use of abbreviations, designations (e.g., incorporated, limited, association), commas, periods, articles, and a lack of standardization regarding how surnames and addresses were captured. These issues were attributable to the absence of a standard naming convention for the VMF.

The audit also found that there was no documented guidance on whether vendors should be setup as temporary or active. Vendor parameters such as vendor status and vendor class could also be captured through a standard naming convention.

ii) Vendor Deactivation/Archiving Procedure

To prevent fraudulent or erroneous payments from being created, it is best practice that vendors are deactivated and archived after a predetermined length of inactivity. Generally, periods between 12 and 48 months of inactivity would trigger the vendor deactivation process. Best practice suggests that companies start as high as 48 months and then progressively reduce that number down until it aligns with the organization. Our review noted that the City had not developed criteria of when to make a temporary or active vendor inactive or when to archive an inactive vendor. Developing criteria for these processes would help guide employees in their duties and help ensure consistency.

Similarly, there was no formulized process setup where employee vendors are deactivated and archived when they terminate employment with the City. A formalized process, whereby Human Resources notifies Financial Services of terminated employees, would ensure employee vendors are deactivated on a timely basis and further improve the accuracy of the VMF.

iii) Cleaning of records and scheduled maintenance procedure

Scheduled maintenance procedures for the VMF include identifying vendors with missing information, removing duplicate vendors and former employees, and inactivating dormant vendors. Best practice suggests that these procedures should be carried out on a periodic basis and that the nature and timing of the procedures are formally documented. Our review noted that the City does not have formally documented procedures for scheduled maintenance of the VMF.

Recommendation 1.6

i) Management should ensure that a consistent data entry format, including standardized naming conventions and required mandatory information, is developed, documented, and implemented for the VMF.

ii) Management should develop a procedure outlining internal criteria regarding if vendors should be setup as temporary or active. Additionally, criteria should also be developed of when to make a temporary or active vendor inactive, and when to archive an inactive vendor.

iii) Management should ensure that terminated employees are removed from the VMF in a timely manner. To achieve this, a procedure should be developed with Human Resources whereby Financial Services is notified of all employee terminations on a scheduled basis.

iv) Scheduled maintenance procedures should be developed and implemented for the VMF. Periodic maintenance should include procedures that ensure the accuracy and completeness of the VMF by identifying vendors with missing information, removing duplicate vendors and former employees, and inactivating dormant vendors.

Management Response and Action Plan 1.6

Operating procedures will be developed during 2021.

Conclusion 1.6

The recommendation will be implemented as stated above.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: December 2021

Information Only: DCM, Finance and Administration

Issue 1.7 - Monitoring and Compliance

Management monitoring programs enable management to continually review business processes for adherence to and deviations from their intended levels of performance and effectiveness. Such monitoring programs are frequently used by organizations to monitor the overall health of the VMF and whether it is trending in the right direction. VMF monitoring generally includes:

- an analysis of the growth/shrinkage of the VMF year over year, including underlying data such as the number of vendors activated and deactivated during the year.
- reviewing audit logs to identify unusual master data changes.
- reviewing user access lists to ensure accuracy.
- monitoring compliance with policy and ensuring that scheduled maintenance procedures are being carried out.

Management indicated that neither Financial Services or Supply Chain actively monitors the VMF or performs any analysis or compliance measures. This can result in inefficiencies in accounts payable and procurement as well as increase the risk of errors or fraud going unnoticed.

Recommendation 1.7

Management should develop and implement a management monitoring process to ensure the accuracy and validity of the VMF. The process should include the calculation of various VMF metrics to assess the health of the VMF, a review of audit logs to identify unusual master data changes, analyzing EFT uptake and trends, reviewing user access rights, and monitoring compliance with policy and procedure.

Management Response and Action Plan 1.7

Operating procedures will be developed during 2021.

Conclusion 1.7

The recommendation will be implemented as stated above.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: December 2021

Information Only: DCM, Finance and Administration

Section 2 – Electronic Funds Transfer (EFT)

Issue 2.1 - Authorization and Review

The Accountant uses information from EFT forms to update banking details for vendors in the Microsoft Dynamics GP system. After inputting the information, the Accountant signs the EFT form and submits it to the Financial Services Manager for review and signoff. Internal Audit reviewed a sample of EFT forms during the audit and noted that all forms were appropriately signed off by the Manager.

Additionally, the Manager also runs an EFT Audit Trails report in GP that produces the banking information and other EFT details that have been entered in the VMF. During this process, the Manager verifies that the information on the form matches the information entered into GP. Management indicated that this process is normally performed every few weeks but sometimes the time interval can be longer.

Best practice suggests that EFT information should be authorized and reviewed prior to being made active in the VMF. This was not occurring at the City as any changes to banking information made by the Accountant were effective immediately, prior to management review. Consequently, the risk of invalid, incomplete and/or inaccurate details being captured in the VMF is increased.

However, because banking details are captured in a vendor’s card in the VMF, the previously discussed vendor approval workflow feature (see Issue 1.1) would apply to EFT changes as well. The implementation of this workflow would ensure that the Manager is made immediately aware of any changes to banking information, and such changes would have to be approved before taking effect.

Recommendation 2.1

Management should implement the vendor approval workflow feature in the Microsoft Dynamics GP system to ensure all EFT detail changes are adequately authorized and reviewed prior to being made active. If this is not possible, all requests for EFT set up or changes to EFT banking information should still be authorized and reviewed by a responsible employee prior to being changed in the VMF.

Management Response and Action Plan 2.1

Management worked with Information Services to test the approval workflow feature in Microsoft GP. As the GP application is hosted in a Citrix environment and the required email client is hosted on local computers, there is no practical implementation method for this approach. Changes to EFT details are reviewed before payment is processed by RBC. There is also a report listing all EFT changes which is reviewed by management.

Conclusion 2.1

Management indicated the recommendation could not be implemented due to technological limitations and therefore the risk of invalid, incomplete and/or inaccurate details being captured in the VMF remains. However, management highlighted detective controls that are in place such as management review of EFT changes. While not as strong as preventive controls, these detective controls help decrease this risk.

Action By: Manager, Financial Services **Action Date**: Complete

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Issue 2.2 - Password

Since EFT bank details are captured within a vendor's card, Microsoft Dynamics GP generally allows those with access to the VMF to also access vendor banking information. The City identified this as an issue and implemented a password to restrict access to the EFT details. Internal Audit reviewed EFT audit logs and determined that only authorized individuals had accessed EFT information since the password was implemented in 2018. The City should be commended for being proactive and implementing this preventive control.

However, discussions with Management indicated that the EFT password had not been changed since it was implemented, thereby increasing the risk of inappropriate user access.

Recommendation 2.2

The password to the “vendor EFT bank maintenance” window, which is needed to access and change vendor banking details, should be regularly changed to protect against unauthorized access.

Management Response and Action Plan 2.2

Management will implement a process to change EFT password on a frequency which addresses operational needs and changes in staff responsibilities.

Conclusion 2.2

The recommendation will be implemented as noted above.

Action By: Manager, Financial Services **Action Date:** February 2021

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Issue 2.3 - Validation and Related Segregation of Duties

Management indicated that the Accountant validates EFT banking information for purchasing vendors prior to entering it into Microsoft Dynamics GP. The validation process generally involves calling the vendor directly from an independently obtained phone number (e.g., from the internet) and validating the EFT request. If the EFT request is for a change in banking details, the old banking details are also requested to ensure the request is legitimate. However, this validation process was not formally documented, which increases the risk of the process being completed erroneously or not at all.

Furthermore, the above validation process was not performed for employee vendors. Although all vendor EFT setups and changes require the submission of a void cheque, it is best practice that all vendors, regardless of type, are independently validated.

The audit also identified internal control weaknesses regarding the validation process. Foremost, the Accountant both validates EFT requests and enters EFT details in the VMF. Therefore, there is a risk this person could perpetrate a fraud by falsely validating a vendor's bank details and instead enter personal banking details in the VMF, thereby redirecting vendor payments. This scheme may go undetected until after payment is made and hence it is important that EFT validation is performed by a person who cannot edit the VMF.

Additionally, the Financial Services Manager could also edit EFT details. This is a concern given that the same Manager is responsible for reviewing EFT data changes. This creates a risk that the Manager could fraudulently change EFT details without anyone else knowing.

Recommendation 2.3

i) Management should ensure that all vendor EFT information is validated for legitimacy prior to setting up or amending a vendor.

ii) Management should ensure that EFT validation is documented for each vendor and that the documentary evidence is reviewed and maintained.

iii) Management should ensure that the person responsible for validating the EFT data cannot also edit EFT details. Likewise, management should ensure that the Financial Services Manager, who is responsible for reviewing EFT data changes, cannot edit EFT details. The Manager should have read-only access which would still allow them to approve VMF and EFT changes via the vendor approval workflow.

Management Response and Action Plan 2.3

i) EFT information for “purchasing” vendors is currently validated for legitimacy prior to set up or amending. There are times when confirming by telephone proves to be nearly impossible and other means are used to determine legitimacy, i.e.: source of information, relationship with vendor, etc. This is a rare occurrence and is discussed with senior management prior to making the determination. EFT information for employee vendors is validated only when a change request is received.

ii) EFT validation is noted on the enrollment form and/or EFT review summaries.

iii) Segregation of duties have been established to the greatest extent possible recognizing operational limitations. Detective measures are in place to ensure staff are only making changes to vendor master file as authorized. Further changes will be considered to improve controls around segregation of duties.

Conclusion 2.3

Management indicated that recommendation 2.3(i) has been partially implemented. EFT information for employee vendors is not validated upon initial setup but rather only when a change request is received. However, there are other controls in place, such as the requirement of a void cheque to initiate an EFT setup, which reduces the likelihood of a fraudulent employee being setup for EFT.

Management indicated that recommendation 2.3(ii) has been implemented as noted above. The extent that management is documenting, reviewing, and maintaining evidence of EFT validation will be reviewed through follow-up work.

Management indicated that recommendation 2.3(iii) has been implemented to the greatest extent possible recognizing operational limitations. As such, duties have not been completely segregated. However, management indicated there are detective controls in place which would help detect fraudulent activity if it were to occur.

Action By: Manager, Financial Services **Action Date:** Complete

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Issue 2.4 - Payment File Upload

Generally, an Accountant in Financial Services generates the EFT payment file from Microsoft Dynamics GP and also completes the upload to RBC Express. Prior to upload, the file from Microsoft Dynamics GP is automatically saved on the City's finance drive as a text file. The text file includes vendor payment amounts and bank account information. While the file contains lines of electronic text and special characters, a person familiar with the file format could potentially alter the file and input fraudulent banking information. Additionally, this payment file is not reviewed or signed off on prior to upload which further increases the risk of fraud.

Ideally, the EFT file would be secure and non-editable. It would also be reviewed and approved before upload to RBC Express. Discussions with those involved with the EFT upload process indicated that there is an approval function available in RBC Express that would require the EFT payment file to be approved before it can be successfully uploaded. This would more closely follow best practice and help to decrease the risk of error or fraud.

Recommendation 2.4

i) Management should implement approval rules in RBC Express so that management must approve the release of EFT funds and related changes to the EFT file.

ii) If the text file cannot be secured, management should review the uploaded text file in detail to ensure it matches the file saved on the network. Management should also confirm that the network file has not been modified since being generated from Microsoft Dynamics GP. This can be done by viewing the "properties" of the text file and verifying that the created date is the same as the modified date. While this review process may be time intensive, it would be needed to fully mitigate the risk that the text file was fraudulently altered.

Management Response and Action Plan 2.4

i) As text files cannot be secured management does not see a practical way to implement this change without significant operational delays as there is no way to verify potentially hundreds of transactions in a text file.

ii) As per above, text files cannot be secured. Employees responsible for uploading the file to RBC Express must have access to the file location and the file in order to perform the upload. Management will continue to explore options on how to validate the uploaded file is the file created in GP.

Conclusion 2.4

The recommendations will not be implemented due to operational requirements and therefore the risk of inserting a fraudulent transaction into the text file remains. However, management has committed to exploring other options on how to validate the uploaded file and will attempt to develop additional procedures as operating policies are developed.

Action By: Manager, Financial Services **Action Date:** On-going

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Issue 2.5 - Reconciliation and Segregation of Duties Issues

Each morning the overnight disbursements are reconciled via the “AP auditors bank reconciliation”. The reconciliation is done in part using an output file from RBC Express that is imported into Microsoft Dynamics GP. Any overnight EFT disbursements are reconciled during this process.

Management indicated that generally the Accountants in Financial Services take turns completing this reconciliation. Consequently, it is possible that the person performing the reconciliation could have also uploaded the EFT file for payment. Given the inherent risk of fraud regarding the text file and upload process as outlined in Issue 2.4, the person who is uploading the file should not be involved in the corresponding reconciliation process.

Additionally, Internal Audit confirmed that unlike the file upload process, there is no procedure outlining how to perform the reconciliation. Given its importance, a formally documented reconciliation process would be an asset.

Recommendation 2.5

i) Management should ensure that the person uploading the EFT text file to RBC Express does not perform the corresponding AP Disbursement Auditor bank account reconciliation if it includes the uploaded EFT transactions.

ii) Management should develop procedures outlining how to perform the AP disbursement auditor bank account reconciliation to ensure the reconciliation is performed correctly.

Management Response and Action Plan 2.5

i) Responsibility for the AP Disbursement Auditor reconciliation will be reassigned to ensure those uploading the EFT file are not performing the reconciliation.

ii) Management will develop procedures around EFT file upload and AP Disbursement Auditor reconciliation.

Conclusion 2.5

The recommendations will be implemented as stated above.

Action By: Manager, Financial Services **Action Date:** December 2021

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Issue 2.6 - Monitoring

Best practice states that EFT monitoring should be an ongoing process that involves procedures to ensure the accuracy and validity of EFT details. This process typically involves scheduled reviews to identify red-flag data changes such as changes and change backs to banking details, analyzing, and working to increase EFT usage for vendors and overall compliance with policy. Furthermore, to mitigate the risk of self-review and potential fraud, monitoring programs require an appropriate segregation of duties.

The audit indicated that there was no formulized EFT monitoring program implemented at the City. Although the Financial Services Manager does run Audit Trails reports to verify the accuracy of EFT data, the frequency and process of the review was not formally documented. In addition, the Manager could change EFT information which does not provide an adequate segregation of duties. As such, the risk of errors or fraud going undetected is increased.

Recommendation 2.6

Management should develop and implement a formal, documented management monitoring process to ensure the accuracy and validity of EFT details. The process should include scheduled reviews of EFT banking changes using the Audit Trails functionality in Microsoft Dynamics GP. Red-flag data changes, such as changes in banking details and change backs, should be identified, and followed up on. The person responsible for reviewing Audit Trails should not have the ability to change EFT information. Additionally, the monitoring process should include an analysis of EFT usage for vendors and overall compliance with policy.

Management Response and Action Plan 2.6

Monitoring of EFT banking changes and additions are currently performed weekly. EFT processes will be documented as part of vendor master file procedures to be completed in 2021.

Conclusion 2.6

The recommendation will be implemented as stated above.

Action By: Manager, Financial Services **Action Date:** December 2021

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Issue 2.7 - Policy and Procedure

The audit determined that the processes of adding a vendor and generating the EFT payment file were outlined in work-flow documents. These documents generally included "how-to" screenshots of the related activity and corresponding explanatory notes. Management should be commended for having workflows outlining these important activities.

However, additional policy and procedure should be developed and implemented to govern EFT activities, as no formal EFT policy was in effect at the City. Therefore, important processes such as EFT authorization, review, validation, and monitoring were not documented, and roles and responsibilities were not formally defined. This lack of policy can cause accountability and efficiency issues.

Recommendation 2.7

Management should develop and implement formalized EFT policy and procedures to ensure consistency of EFT practices and establish accountability. Processes such as EFT authorization, review, validation, and monitoring should be documented, and related roles and responsibilities should be formally defined in policy.

Management Response and Action Plan 2.7

Operating procedures will be developed during 2021.

Conclusion 2.7

Management intends to resolve this issue through the development of operating procedures. Management also indicated during subsequent discussions that they will develop a formal policy as time and resources permit.

Action By: Manager, Financial Services **Action Date:** December 2021

Information Only: DCM, Finance and Administration
Manager, Supply Chain

Section 3 – Wire Transfer Payments

Issue 3.1 - System Administration

A listing of access rights for the RBC Express wire transfer payment service was obtained during the audit indicating that the Manager of Financial Services, Manager of Budget & Treasury, and the Deputy City Manager of Finance & Administration are administrators on the system. Administrators have permissions on all accounts and therefore it is possible for an administrator to both create a wire transfer payment and approve a wire transfer payment. However, due to the dual approval function for wire transfer payments, any wire transfer payment initiated and approved by an administrator would need approval from a second approver.

Nevertheless, this control could be overridden as audit testing showed that administrators could independently change the system from dual approval to single approval. Therefore, there is a risk that an administrator could change the approval rules to a single approver and then initiate and approve a fraudulent payment. Given that many of the wire transfer payments exceed a million dollars, this is a significant risk for the City.

Internal Audit determined that there may be a dual administration feature available in RBC Express. This control, when activated, would require a second administrator to approve another administrator’s changes, thereby significantly strengthening internal controls.

Recommendation 3.1

Management should contact RBC and if possible, setup dual administration in RBC Express. Dual administration requires a second administrator to approve another administrator’s changes (i.e., changing from dual approval to single approval), thereby significantly strengthening internal controls.

Management Response and Action Plan 3.1

Dual administration has been set up on RBC Express, all changes now require dual approval.

Conclusion 3.1

Management indicated that the recommendation has been implemented as stated above.

Action By: Manager, Financial Services **Action Date:** Complete

Information Only: DCM, Finance and Administration
Manager, Budget and Treasury

Issue 3.2 - System Access and Segregation of Duties

Our review of access rights for the wire transfer payment service identified additional access and segregation of duties issues. The review determined that a Supervisor in Payroll had access to both initiate and approve wire transfer payments. This is not in line with best practices which state that employees should not have the ability to approve their own transactions. Subsequent follow-up also indicated that this person was no longer involved in the wire transfer payment process and did not utilize wire transfer payments in their current role. Consequently, the Supervisor does not require access rights to the wire payment service.

Recommendation 3.2

i) Management should review employee access rights in RBC Express to ensure an appropriate segregation of duties is implemented. Employees should not have the ability to both create and approve a wire transfer payment.

ii) Management should review employee access rights in RBC Express to ensure they are appropriate. Employees, such as the Payroll Supervisor, should not have access to wire payments in RBC Express if they do not require it to perform their job duties.

Management Response and Action Plan 3.2

Management is in the process of reviewing all employees set up in RBC Express and their access. Changes will be made to ensure compliance to this recommendation.

Conclusion 3.2

The recommendations will be implemented as stated above.

Action By: Manager, Financial Services **Action Date:** June 2021

Information Only: DCM, Finance and Administration
Manager, Budget and Treasury

Issue 3.3 - Wire Transfer Payment Documentation and Review

Audit testing included recalculating sampled wire transfer payments and requesting supporting documentation for the payments. While management was able to provide documentation verifying the accuracy of payment amounts, it was difficult for management to provide supporting data for the accuracy of banking details related to individual wire transfer payments. In one instance management was unable to provide acceptable documentation regarding wire bank details of a recurring payee. While absolutely no fraudulent activity was suspected, it did highlight the need for better documentation regarding wire transfer payments.

Unlike the EFT process, wire transfer payees were not supported by any standardized form. Instead, wire transfer payments were generally made via a template in RBC Express. Templates capture payee information such as name, banking details, routing number, etc. and the information is saved within RBC Express for future recurring use. Templates, when initially setup, must be approved by an approver within the system.

Our review noted that many of the templates were setup a number of years ago and lack adequate documentation, thereby increasing the risk of inaccurate and/or fraudulent payment. The development of a standardized wire authorization form, similar to the EFT form, would help mitigate these risks as it could capture pertinent wire transfer payment details. Such details could then be used to create payee templates, with the form acting as a supporting document for the template. The forms would require independent validation like the EFT process, and also require management review when approving templates.

Furthermore, system access reports showed that some wire transfer payment users could create non-recurring wire payments. These non-recurring payments do not use a historical template to facilitate payment. Instead, the user themselves enters the pertinent wire transfer payment details including bank account information. As such, there was a risk that a user may initiate a fraudulent payment into a personal bank account but disguise it as a legitimate recurring payment. Removing the ability to create non-recurring wire transfer payments, and also ensuring all wire payments are made via preapproved templates, would mitigate this risk.

In addition to the standardized forms, it is best practice that documentation showing the accuracy and validity of each wire transfer payment is provided to the approver for review. Management indicated that this was not always happening due to the nature of the recurring wire transfer payments. Consequently, the risk of making an inaccurate or invalid payment was heighted. Ensuring that adequate documentation is provided to approvers would help reduce these risks and also strengthen the audit trail.

Recommendation 3.3

i) Management should develop and implement a wire authorization form, similar to the EFT form, to formally document wire details (e.g., bank account number, routing #, etc.) for each payee. Information in the wire authorization form should be used to create payee templates in RBC Express. Prior to template approval, these forms should be reviewed by management and validated for legitimacy by an employee who cannot initiate a wire payment.

ii) Management should ensure that all wire payments are made via template and template details are supported by the wire authorization form.

iii) Management should review its template listing to ensure that all templates are actively being used. Any template that is no longer active should be deleted.

iv) To ensure accuracy and protect against possible fraudulent payments, management should ensure approvers review appropriate supporting documentation before approving wire transfers and that the documentation is retained for audit purposes.

Management Response and Action Plan 3.3

i) Management will ensure validation of the source document prior to setting up a wire template in RBC Express.

ii) As part of recommendation 3.2 employee access rights will eliminate the ability to create wires without using a template.

iii) Review of templates has been completed and any no longer being used have been deleted.

iv) Schedule of recurring wire payments is prepared annually and used by employee preparing the transfer as well as the approver as supporting documentation. Management will ensure supporting documentation will be provided to the approver for verification.

Conclusion 3.3

The recommendations will be implemented as stated above.

Action By: Manager, Financial Services **Action Date:** June 2021

Information Only: DCM, Finance and Administration
Manager, Budget and Treasury

Issue 3.4 - Summary Reports

Scheduled review of summary payment reports is a best practice detective internal control that is typically part of the wire payment process. These summary reports, which outline all of the wire payments transferred during a given period, are usually reviewed, and approved by a manager high enough in the division to act upon any noted issues. However, to ensure an adequate segregation of duties, the manager does not have the ability to approve wire transfer payments. Detective internal controls such as this are especially relevant if there is a breakdown in preventive controls.

Discussions with management during the audit determined that summary reports were not reviewed in relation to wire payments. This increases the risk that errors or fraud may go undetected.

Recommendation 3.4

Management should ensure that monthly summary reports are prepared with respect to wire transfers paid. These reports should be reviewed and signed off by a senior finance official who does not have the ability to approve wire payments and be retained for future reference. Any identified irregularities should be immediately investigated.

Management Response and Action Plan 3.4

A monthly summary report of wire payments will be prepared by Manager, Budget and Treasury, and submitted for review and sign off by the DCM, Finance and Administration. To ensure proper segregation of duties, the DCM, Finance & Administration will be removed from the approval queue for approval of wire payments, except for when required as back up in circumstances when one of the other three approvers is unavailable.

Conclusion 3.4

Management indicated that the recommendation has been implemented as stated above.

Action By: Manager, Financial Services **Action Date:** Complete

Information Only: DCM, Finance and Administration
Manager, Budget and Treasury

Issue 3.5 - Wire Transfer Policy and Procedure

Best practice suggests that wire transfer payment policies and/or procedures be robust enough to provide direction to employees on all aspects of the wire transfer payment process. This would normally include formally defining the roles, responsibilities, and processes of the wire transfer payment activity in a written document that is available to all employees involved in the process.

Discussions with management determined that there is no policy or procedure in place regarding wire transfer payments. Lack of formal policy and/or procedures can increase the likelihood of errors and fraudulent activity and are critically important due to the large dollar value of some of the wire transfer payments made at the City.

Recommendation 3.5

Management should develop policies and procedures that guide employees and provide direction on all aspects of completing a wire transfer payment. Areas such as usage, initiation and review, authorization limits, approval rules and related controls should be documented.

Management Response and Action Plan 3.5

Operating procedures will be developed during 2021.

Conclusion 3.5

Management intends to resolve this issue through the development of operating procedures. Management also indicated during subsequent discussions that they will develop a formal policy as time and resources permit.

Action By: Manager, Financial Services **Action Date:** December 2021

Information Only: DCM, Finance and Administration
Manager, Budget and Treasury

Issue 3.6 - Wire Transfer Payments for Vendors

To help maintain efficiency in the accounts payable process, vendors should be paid by EFT wherever possible. Through discussions with management the audit determined that a small number of vendors were typically paid by wire transfer instead of cheque or EFT. Management indicated that this is sometimes required when payment must be made to a vendor in a foreign currency. However, management also noted that it may be possible to transition some vendors paid by wire transfer to EFT payment.

Additionally, the audit identified that wire transfer payments were not included in the weekly payment vouchers that are approved during regular City Council meetings and as a result these payments were not being formally approved by Council.

Recommendation 3.6

i) Management should identify vendors that are paid by wire transfer, and if possible, transition payment to these vendors to electronic funds transfer.

ii) Management should ensure that wire payments are included on the weekly payment vouchers listing that is approved during the regular City Council meeting.

Management Response and Action Plan 3.6

i) Any vendors previously paid by wire have been transitioned to EFT. Only in extenuating circumstances do we send vendor payment using wire transfer.

ii) When monthly summary report of wire payments is reviewed and signed off by DCM, Finance and Administration (recommendation 3.4), the total monthly wires will be added to the next weekly payment voucher listing to be approved during regular City Council meeting.

Conclusion 3.6

Management indicated that the recommendations have been implemented as stated above.

Action By: Manager, Financial Services **Action Date:** Complete

Information Only: DCM, Finance and Administration
Manager, Budget and Treasury

Section 4 – Other Issues

Issue 4.1 - Fraud Training

During the audit, several tests were performed in an effort to identify any fraudulent vendors or activity. These procedures did not identify any VMF, EFT or wire transfer payment activity that would be indicative of fraud. However, through discussions with management, it was determined that employees involved with these processes had not received adequate fraud training.

Large frauds have recently happened in other Canadian municipalities[1] with losses of over $1M being reported. These frauds involved phishing schemes that resulted in fraudulent wire transfers or EFT payments. Many of these phishing schemes share similar characteristics and therefore employee training on certain red flags that may be indicative of fraud would be beneficial. Providing such training to all employees involved with vendor management, EFT and wires would mitigate the risk of a similar fraud occurring at the City.

Recommendation 4.1

Training related to how to identify and protect from potential phishing attacks and other fraud schemes related to VMF, EFT and wire transfer payment processes should be provided to all employees involved in these processes.

Management Response and Action Plan 4.1

Appropriate training will be sought and provided where feasible.

Conclusion 4.1

The recommendation will be implemented as stated above.

[1] The cities of Ottawa, Burlington and Saskatoon fell victim to phishing schemes in 2019.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: September 2021

Information Only: DCM, Finance and Administration

Issue 4.2 - Vendor Forms

A number of forms were utilized in relation to the VMF and EFT processes. These included the vendor add/change form used by Supply Chain, the cheque requisition form, the vendor EFT form, and the employee EFT form.

The audit identified possible areas of improvement for each form, however, management should consider combining all of the forms into one standardized vendor form. This would improve the vendor addition/change process by:

- Increasing the accuracy and completeness of the VMF by ensuring pertinent vendor details are obtained for all vendors.

- Making the process more streamlined and efficient for vendors as they only have to complete a single form.

- Improving the audit trail in that all vendors have supporting vendor forms.

- May increase EFT uptake for vendors, especially those vendors who receive one-time payments. The audit noted that only 1 percent of vendors setup in 2019 receiving one-off payments received payment by EFT.

- Reducing the overall number of paper forms used.

Recommendation 4.2

Management should consider developing a new standardized vendor form that can be used to capture information, including EFT information, from all types of vendors. Additionally, the following best practices should be considered when developing a new vendor form:

- The form should reference section 61(c) of the Access to Information and Protection of Privacy Act, 2015, which outlines a public body can collect personal information for the purpose of making a payment.

- The form should plainly state that vendor details will be validated, as this may dissuade fraudsters from submitting fraudulent EFT forms.

- The form should have an internal section noting that the vendor information has been validated and by whom.

- The form should clearly request direct contact information (e.g., a direct phone number instead of a general business phone number).

- The vendor completing the form should be required to sign and date the form.

- A “responsibility of the vendor” or similar disclaimer should be on the form that notes a supplier is required to notify the City promptly should vendor information change. The disclaimer should also note that the City will not be responsible for lost or delayed mail where address changes were not communicated in a timely manner.

- The form should require both the employee who enters the data in the VMF and the reviewer to sign and date the form.

- The form should be accompanied by detailed instructions explaining the different sections of the form and how to complete them.

- The form should request HST/GST registration numbers to ensure the validity of the City's input tax credit claims.

Management Response and Action Plan 4.2

As part of a current CI project on procurement and requisitioning goods/services management has developed updated vendor forms for procurement vendors and EFT information.

A vendor form will not be required for non-purchasing type vendors i.e.: employees, refunds to individuals or businesses, legal claims, grants. The vendor detail for these type vendors comes from the expense claim or cheque request form.

Conclusion 4.2

Management indicated that the recommendation has been implemented. Although all of the information has not been consolidated into a single form as suggested in the recommendation, management stated that the forms were reviewed, and that the purchasing vendor form and the EFT form have been updated.

Action By: Manager, Financial Services
Manager, Supply Chain

Action Date: Complete

Information Only: DCM, Finance and Administration