Accounts Payable Access to Vendor Master File

Internal Audit Report

November 14, 2017

Internal Audit
Orange County Public Schools

Linda J. Lindsey, CPA, CGAP, Senior Director
Jan N. Skjersaa, CPA, Internal Auditor
Alpa H. Vyas, CIA, CRMA, Internal Auditor

Table of Contents

EXECUTIVE SUMMARY

Why We Did This Audit

The risk assessment process highlighted that the Accounts Payable Department has access to certain fields in the Vendor Master File (VMF), raising segregation of duties concerns.

The objective of this audit was to determine who has what access to the VMF and whether compensating controls exist over access to the VMF by Accounts Payable staff to mitigate the lack of proper segregation of duties that should be present in an effective internal control system.

This audit was included in the 2016-2017 Annual Audit Plan.

What We Found

Our overall conclusion is that some controls are in place while other controls are missing or inadequate. We found: 1) the Accounts Payable staff has the ability to process payments to vendors and to modify information in the VMF; 2) no department takes responsibility for the bank details field in the VMF; 3) the old and new values of the bank details field do not show in the Change Log; and, 4) several users have access to critical SAP transaction codes MK05 - Purchase Block/Unblock Vendor - and XK05 - Purchase and Posting Block/Unblock Vendor.

What We Recommended

- The ability to access and change sensitive VMF fields should not be performed by persons involved with processing of vendor payments
- The VMF Change Log should record both the old and new values of the bank details field
- Management should establish ownership of the bank details field in the VMF
- Analysis and evaluation are needed to correct the PRAA users list and to properly limit access to bank details to only those persons who need it to perform their job responsibilities
- Access to employees' sensitive information should be limited to those who have a need
- There should be a formal written policy and procedure for monitoring the Change Log
- Access to change a vendor name should be limited. Any changes to the vendor name in VMF should require approval by an authorized individual
- A VMF transaction code review process should be established and implemented quarterly by BPSs, users, and IT Security

This report has been discussed with management and they have prepared their response which follows.

BACKGROUND:

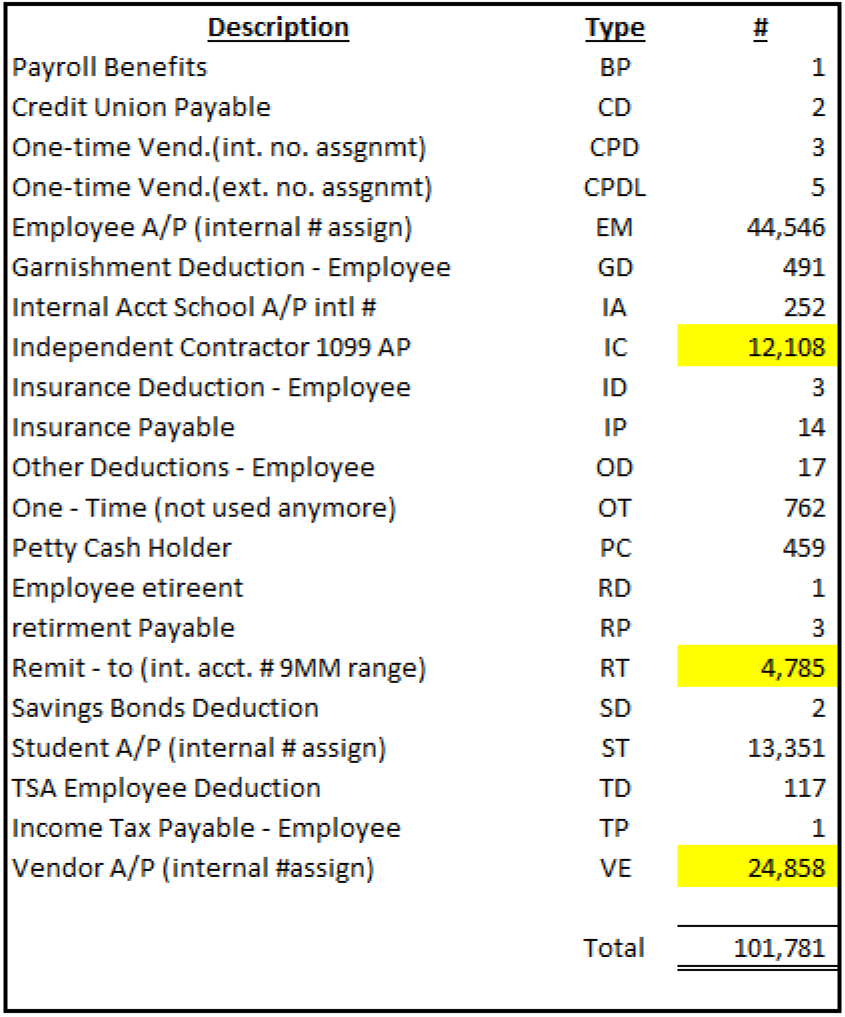
The Vendor Master File (VMF) is a primary element of the Procurement and Accounts Payable operations. The VMF contains significant information of Orange County Public Schools' (OCPS) vendors and related transactions for procurement of goods and services.

Maintenance and safeguarding of the VMF are essential in order to avoid unauthorized, inappropriate, or duplicate transactions and to meet the district's objective of efficient operations.

Maintenance and safeguarding of the VMF are essential.

There are several types of vendors in the VMF.

Table 1: Quantity of Vendor Types (as of 07/12/2017)



Description	Type	#
Payroll Benefits	BP	1
Credit Union Payable	CD	2
One-time Vend.(int. no. assgnmt)	CPD	3
One-time Vend.(ext. no. assgnmt)	CPDL	5
Employee A/P (internal # assign)	EM	44,546
Garnishment Deduction - Employee	GD	491
Internal Acct School A/P intl #	IA	252
Independent Contractor 1099 AP	IC	12,108
Insurance Deduction - Employee	ID	3
Insurance Payable	IP	14
Other Deductions - Employee	OD	17
One - Time (not used anymore)	OT	762
Petty Cash Holder	PC	459
Employee etireent	RD	1
retirment Payable	RP	3
Remit - to (int. acct. # 9MM range)	RT	4,785
Savings Bonds Deduction	SD	2
Student A/P (internal # assign)	ST	13,351
TSA Employee Deduction	TD	117
Income Tax Payable - Employee	TP	1
Vendor A/P (internal #assign)	VE	24,858
	Total	101,781

Source: Vendor Master records downloaded on 07/12/2017 from the SAP ZVendor_report, then summarized by type using IDEA application.
Prepared by: Internal Audit

There are 41,751 Vendor records (types IC, RT, and VE in yellow) that were the focus of this audit.

This audit focused on access to the Vendor A/P vendor master file data in types IC, RT and VE. A diagram showing the process of creating a vendor in the VMF through the payment process is in the Appendix. (See Flowchart 1).

The VMF Change Log recorded 92,828 changes to fields in the VMF during FY 2016-17 (See Table 3 in the Appendix). The VMF Change Log records the date of change, time of change, vendor number, who changed the field, the field name changed, the old field value and the new field value for all fields except those which are considered sensitive. Sensitive fields include the following: bank details, name, individual payment, payment methods, payment terms, clerk's internet address, PO box, vendor status inactive/active, tax number 1 (SSN), and tax number 2 (EIN-Employer Identification Number).

SAP transaction screens allow various levels of access to fields in the VMF. The following table explains the function of each screen and which departments have access to them.

Table 2: SAP Transaction Screens

VMF Transaction	Description	Current Access by Department
FK02	Change Vendor (Accounting)	Accounts Payable and Finance
FK05	Block/Unblock Vendor (Accounting)	Accounts Payable, Facilities, HR, ITS (Infrastructure, Customer Service, Applications, Security, and Business Process Specialists (BPSs)).
MK01	Create Vendor (Purchasing)	Procurement, Business Opportunity & Procurement BPS
MK02	Change Vendor (Purchasing)	Procurement & Business Opportunity, Payroll, and Procurement BPS
MK03	Display Vendor	All departments
MK05	Block/Unblock Vendor (Purchasing)	Finance, Facilities, Communication, HR, ITS (Infrastructure, Customer Service, Applications, Security, and BPSs), OMB, Procurement, and Transportation.
XK01	Create Vendor	Finance, Payroll, Procurement, Business Opportunity, & Procurement Business Process Specialist (BPS)
XK02	Change Vendor	Accounts Payable, Finance, Payroll, Procurement & Business Opportunity, and Procurement BPS
XK03	Display Vendor	All departments
XK05	Block Vendor	Accounts Payable, Finance, Payroll, Procurement & Business Opportunity, and Procurement BPS

Source: SAP transaction screens and information from ITS – Security as of 06/20/2017
Prepared by: Internal Audit

Data fields considered sensitive include:

- *Bank details*
- *Name*
- *Individual payment*
- *Payment methods*
- *Payment terms*
- *Clerk's internet address*
- *P.O. Box*
- *Vendor status*
- *Tax numbers 1 & 2*

OBJECTIVES, SCOPE AND METHODOLOGY:

Objectives

The objective of this audit was to determine who has what access to the VMF and whether compensating controls exist over access by Accounts Payable staff to the VMF to mitigate the lack of proper segregation of duties that should be present in an effective internal control system.

To determine:

- *whether appropriate internal controls exist over access to VMF;*
- *what the access is; and,*
- *whether it is consistent with the segregation of duties that should be present.*

Scope

The scope of the audit included:

- determining what access to the VMF is possible by Accounts Payable and other departments and,
- understanding the reason for access to sensitive fields by those staff members.

Methodology

Our audit methodology included,

- interviewing staffs of Accounts Payable and other departments;
- performing walk-throughs of processes with the Accounts Payable staff and other department staff;
- reviewing the VMF change log for the period of July 1, 2016 to June 30, 2017; and,
- researching best practices.

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

Our audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* of the Institute of Internal Auditors and included such procedures as deemed necessary to achieve the objectives. Internal Auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. We are required to note any material deficiencies in accordance with Florida Statutes, School Board Policy and sound business practices. We also offer suggestions to improve controls or operational efficiency and effectiveness.

FINDINGS & RECOMMENDATIONS:

1) The Accounts Payable staff has the ability to process payments to vendors and to modify information in the VMF. High Risk

Best Practice: Access controls over the VMF strengthen the system. Segregation of duties is critical to effective internal controls. Adequate segregation of duties assists to reduce the risk of inappropriate activities. The staff member who has the ability to process payments to vendors should not also have access to modify information in the VMF.

Audit Finding: Accounts Payable staff can modify the following information in the VMF: bank details, payment methods, and payment terms, and they process vendor payments. There is not adequate oversight or monitoring of such changes, nor are there adequate compensating controls.

Accounts Payable can both process payments to vendors and modify VMF information.

Recommendation: The ability to access and change sensitive VMF fields should not be performed by persons involved with the processing of vendor payments.

2) There is no record of changes to the bank details field in the VMF Change Log. High Risk

Best Practice: A record of changes to sensitive information provides a critical component in fraud detection, error correction, regulatory compliance, and risk management. A record of changes can uncover undesirable acts ranging from innocent mistakes to fraud. When segregation of duties is not achieved, careful review of changes can provide a compensating control to mitigate risk.

There is no record prepared of changes to bank details field in the VMF Change Log.

Audit Finding: The VMF Change Log records the details of changes to the bank details field such as who made the change, date and time of change, and whether the person created or deleted data; however, the

Change Log does not record the old value or the new value of the field. The only bank details retained in the file are the last ones entered. In this case, an unauthorized change to an incorrect receiving account could be entered, posted and then changed back to the correct account without leaving a record of those changes.

Unauthorized changes to vendor banking information could occur and not be detected.

Recommendation: The VMF Change Log should record both the old and new values of the bank details field. This will facilitate a compensating control, assist in the detection of any inappropriate change, and allow for improved monitoring of the VMF.

3) Ownership of bank details data fields in VMF file has not been established. High Risk

Best Practice: Each data field should have an owner – a department or staff member who is responsible for its accuracy and for authorizing and controlling access and changes. Ownership of data fields allows management to assign accountability and resolve problems by contacting the responsible party, the owner. Most commonly, vendor master records are considered to be owned by the procurement function as they maintain and facilitate vendor relationships.

Audit Finding: No department has acknowledged ownership of the bank details fields in the VMF, so accountability is lacking in that area.

No department takes ownership of the bank details data fields in VMF.

Recommendation: Management should establish the ownership of the bank details fields in the VMF. This will improve the effectiveness and efficiency of the operation. Typically the Procurement Department is the owner of vendor master file data.

4) The list of users assigned to use the SAP PRAA screen was not accurate. There were users listed who could not access the PRAA screen. We could not determine if the reverse occurs (whether users who were not on the list have access to the screen). High Risk

Best Practice: A key decision to make during the design of security is whether to use “job-based” or “task-based” roles. Giving the right roles to the right position and/or giving the right access to the right roles is fundamental to access security. An established periodic role and user analysis process can determine if new or existent roles are in compliance with the policies.

Audit Finding: The SAP transaction screen PRAA (Automatic Vendor Maintenance) is a program that can be run as a scheduled batch job to create an Employer Vendor Record from the HR Master Data File.

We obtained a list from the ITS Security staff of the users who have a role with the PRAA transaction assigned to it. The PRAA transaction code provides access to bank details, among other data fields. The list of users we were provided did not reflect accurate information. We found that certain individuals listed as having access to PRAA could not, in fact, access that transaction code. After we informed ITS Security of this finding, they updated the PRAA access list. Members of the travel reimbursement staff from Finance were aware of this transaction and they are the only ones who use it. However, they do not require access to bank details to perform their travel reimbursement function.

The list of users assigned to SAP PRAA transaction screen was not accurate.

Recommendation: Analysis and evaluation are needed to correct the PRAA users list and to properly limit access to bank details to only those persons who need it to perform their job responsibilities.

5) Certain Finance Department staff members are able to view and make changes in bank details information while loading HR Master Data File through the SAP-PRAA transaction for the creation of Employee Vendor accounts for travel reimbursements. High Risk

Best Practice: In today’s environment, it is important to safeguard assets, such as sensitive information, by a good access management system. Staff should have information only on a need–to-know basis. Giving users access to sensitive information that is not needed in the performance of their job creates opportunities for errors and irregularities.

Audit Finding: We were informed by management of the Finance Department that their staff do not create or have access to change bank details; however, the VMF Change Log indicates that Finance staff does create bank details. During our walk-through meeting with the Finance staff we noted that, during the creation of a new employee vendor for reimbursement purposes, staff runs a standard batch program and loads HR Master Data File through the PRAA (Create/Change/Block Vendor Master Records from HR Master Data) transaction code. While loading data from HR Master Data File, staff has to tab through each required screen and submit. Those screens are:

- Create Vendor: Address
- Create Vendor: Control
- Create Vendor: Payment Transactions
- Create Vendor: Contact Persons
- Create Vendor: Accounting Information
- Create Vendor: Payment Transactions Accounting
- Create Vendor: Correspondence Accounting

The system then creates an employee vendor number for reimbursement purposes. Finance staff are able to view and make changes to bank details in the VMF as they perform this process.

Finance staff have the ability to make changes in bank details data fields.

Recommendation: Access to employees' sensitive information should be limited to only by those who have a need. Transaction code PRAA should be modified to prevent access to bank details data fields.

6) No policies and procedures are established for monitoring the bank details fields of the VMF Change Log. High Risk

Best Practice: Monitoring change logs provides important detection controls. There should be a written policy and procedure for monitoring the VMF Change Log.

Audit Finding: Changes in bank details are not monitored.

Recommendation: Periodically reviewing and monitoring the VMF Change Log will assist in identifying inappropriate changes or irregularities in sensitive information. There should be a formal written policy and procedure for this monitoring. This will assist in ensuring consistency in practice as well as when training new employees. The Accounts Payable department's focus should be on changes to bank details data fields.

7) Most of the staff who have access to the VMF can change the vendor's name in VMF without approval. High Risk

Best Practice: Only a few staff should have ability to change data in the VMF records, since the VMF is used for payment processing.

Vendor's name in VMF can be changed without approval.

Audit Finding: Most of the staff who have access to the VMF have the ability to change the vendor name. In addition, the current process of changing the name of a vendor does not require an approval or authorization.

Recommendation: Access to change a vendor name should be limited. Any changes to the vendor name in the VMF should require approval by an authorized individual.

8) Several users have access to transaction codes that are not appropriate for their roles. (MK05 - Purchase Block/Unblock Vendor and XK05 - Purchase and Posting Block/Unblock Vendor) High Risk

Best Practice: Only certain staff should have ability to block or unblock vendors in the VMF. Adequate access controls help to reduce the risk of inappropriate activities.

70 users from 8 different departments had access to transaction code MK05.

Audit Findings: a) A total of 70 users from eight different departments have access to the MK05 transaction code. The MK05 transaction code blocks or unblocks purchasing documents (i.e., requisitions, purchase orders, etc.) from being processed against a vendor. Only certain staff should have access to change MK05 transaction code for operational purposes.

The Change Log 2016-17 indicated that three staff from Procurement and one staff from Finance made changes in MK05. Changes made by the Procurement staff appear to be valid changes. We are not certain about changes made by Finance and question why Finance staff have access to code MK05. A staff member who had transferred from Finance to Communications also had access to MK05 because their role had not been updated to delete access to that transaction after they changed positions.

One Finance staff was moved from Finance to Communications, and still had access to MK05.

After we brought this to their attention, BPS removed staff from MK05 and updated MK05 users list. In reference to other unnecessary access to transaction MK05, Procurement, BPS and IT Security decided to delete MK05 from different roles and to add Procurement's two staff who are authorized to use this transaction code.

IT Security informed us that this modification can be completed in mid-December because Support Packs in the SAP System are in process. Procurement will submit a heat ticket for this modification and after approval of BPS, changes can be effective.

One Finance staff had two roles from Finance as well as one from Procurement, and had access to MK05 and XK05. Finance staff should not have access to either MK05 or XK05.

b) A total of 30 users from six departments have access to XK05 transaction code. The XK05 transaction code blocks or unblocks new invoices and/or purchasing documents (i.e., requisitions, purchase orders, etc.) from being processed against a vendor. Only certain staff should have access to the XK05 transaction code for operational purposes. Change Log 2016-17 indicated that only two staff from Procurement made changes in XK05 and those appear to be valid changes. After our notification, BPS and IT Security updated access to the XK05 transaction code in SAP and updated XK05 users list on 11/6. However, after verification of the updated list dated 11/6, we noted that one Finance staff was also assigned a Procurement role and had access to both XK05 and MK05. This staff member never uses the XK05 transaction code. After we informed them, the Finance BPS removed this Finance staff person from the Procurement role and updated XK05 users list again on 11/9. We confirmed the 11/9 updated XK05 users list.

Multiple revisions to the access list for these transactions were made as audit discoveries were made and ITS Security was notified.

<u>Recommendation:</u> A VMF transaction code review process should be established and implemented quarterly by BPSs, users and IT Security.

We wish to thank the staffs of the Accounts Payable, Procurement, Finance, and IT Security Departments for their cooperation and assistance in the conduct of this audit.

Appendix
Flowchart 1 – Vendor Master File Creation Process

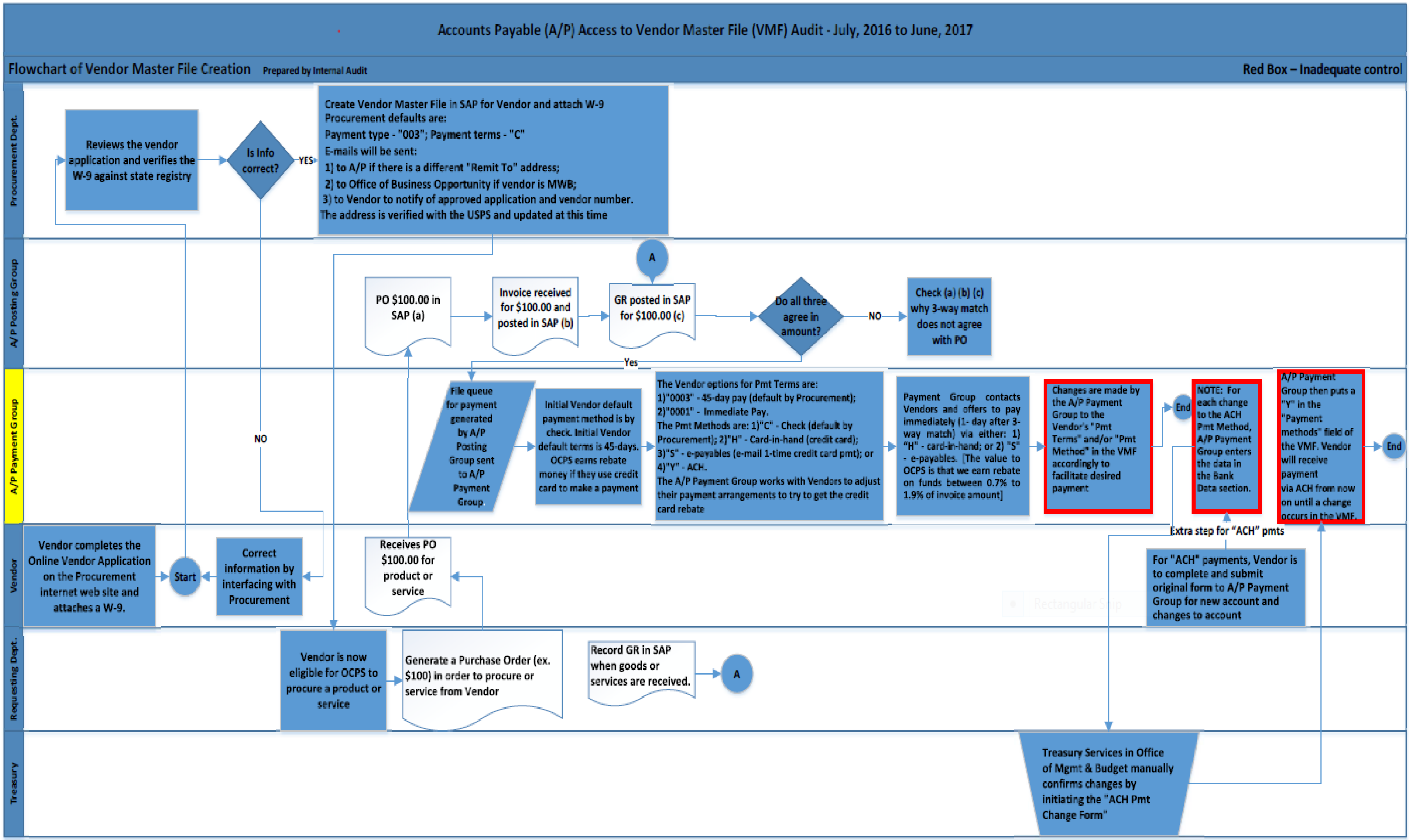

Accounts Payable (A/P) Access to Vendor Master File (VMF) Audit - July, 2016 to June, 2017
Flowchart of Vendor Master File Creation
Prepared by Internal Audit
Red Box – Inadequate control
Procurement Dept.
A/P Posting Group
A/P Payment Group
Vendor
Requesting Dept.
Treasury
Reviews the vendor application and verifies the W-9 against state registry
Is Info correct?
YES
NO
Create Vendor Master File in SAP for Vendor and attach W-9
Procurement defaults are:
Payment type - "003"; Payment terms - "C"
E-mails will be sent:
1) to A/P if there is a different "Remit To" address;
2) to Office of Business Opportunity if vendor is MWB;
3) to Vendor to notify of approved application and vendor number.
The address is verified with the USPS and updated at this time
A
PO $100.00 in SAP (a)
Invoice received for $100.00 and posted in SAP (b)
GR posted in SAP for $100.00 (c)
Do all three agree in amount?
NO
Check (a) (b) (c) why 3-way match does not agree with PO
Yes
File queue for payment generated by A/P Posting Group sent to A/P Payment Group.
Initial Vendor default payment method is by check. Initial Vendor default terms is 45-days. OCPS earns rebate money if they use credit card to make a payment
The Vendor options for Pmt Terms are:
1)"0003" - 45-day pay (default by Procurement);
2)"0001" - Immediate Pay.
The Pmt Methods are: 1)"C" - Check (default by Procurement); 2)"H" - Card-in-hand (credit card);
3)"S" - e-payables (e-mail 1-time credit card pmt); or
4)"Y" - ACH.
The A/P Payment Group works with Vendors to adjust their payment arrangements to try to get the credit card rebate
Payment Group contacts Vendors and offers to pay immediately (1- day after 3-way match) via either: 1) "H" - card-in-hand; or 2) "S" - e-payables. [The value to OCPS is that we earn rebate on funds between 0.7% to 1.9% of invoice amount]
Changes are made by the A/P Payment Group to the Vendor's "Pmt Terms" and/or "Pmt Method" in the VMF accordingly to facilitate desired payment
End
NOTE: For each change to the ACH Pmt Method, A/P Payment Group enters the data in the Bank Data section.
A/P Payment Group then puts a "Y" in the "Payment methods" field of the VMF. Vendor will receive payment via ACH from now on until a change occurs in the VMF.
End
Extra step for "ACH" pmts
Vendor completes the Online Vendor Application on the Procurement internet web site and attaches a W-9.
Start
Correct information by interfacing with Procurement
Receives PO $100.00 for product or service
For "ACH" payments, Vendor is to complete and submit original form to A/P Payment Group for new account and changes to account
Vendor is now eligible for OCPS to procure a product or service
Generate a Purchase Order (ex. $100) in order to procure or service from Vendor
Record GR in SAP when goods or services are received.
A
Treasury Services in Office of Mgmt & Budget manually confirms changes by initiating the "ACH Pmt Change Form"

Table 3: List of Fields That Changed and How Many Times

Field Name	# of Changes
Account memo	452
Acctg clerk	65
Act.clk tel.no.	452
Aut. GRSet Ret	1
Automatic PO	26
Bank Details	3,038
Block function	823
Building Code	1
BusinessPartner	1,389
Certifictn Date	1
City	1,785
Clerk at vendor	559
Clerk's fax	409
Clrk's internet	402
Cntrl Addr.Admn	7,314
Co.cde deletion flag	8
Co.code post.block	474
CoCd del.block	8
Comm. Method	338
Company code data	3,612
Control key	4
Country	1,531
Data line	8,098
Del. flag POrg.	9
Deletion block	964
Deletion flag	1,583
District	235
E-Mail Address	1,698
Extension	82
Fax	638
Fax Number	1,006
First name	1,389
GR-Based IV	27
General data	3,608
Head office	279
Home address	150
House Number	18
Individual pmnt	40
Language	1,429
Last name	1,389
Local process.	1
Minority indic.	3
Mobile phone	147
Name	2,675
Name 2	878
Order currency	1
P.O.Box city	15
PO Box	154
PO Box City	12
PO Box PCode	290
PO Box Pstl Cd	290
Partner Role	1,645
Payment methods	2,021
Payt Terms	2,840
Personnel No.	53
Planning group	6
Postal Code	5,472
Posting Block	2,795
Prev.acct no.	3
Pur. block POrg	8
Purch. block	910
Purchasing Data	1,777
Recon. account	929
Region	158
Salesperson	163
Search Term	3,794
Search Term 2	995
Search term	3,662
Sort key	73
Standard No.	8
Street	4,331
Street 4	37
Tax Number	109
Tax Number 2	156
Telebox	326
Telephone	1,794
Telephone	168
Telephone	2,388
Telephone 2	10
Time zone	214
Title	1,389
Tolerance grp	5
URL	1,492
W. Tax Code	2,277
TOTAL	**92,828**

Source: VMF Change Log 2016-17

Table 4: Roles by Department

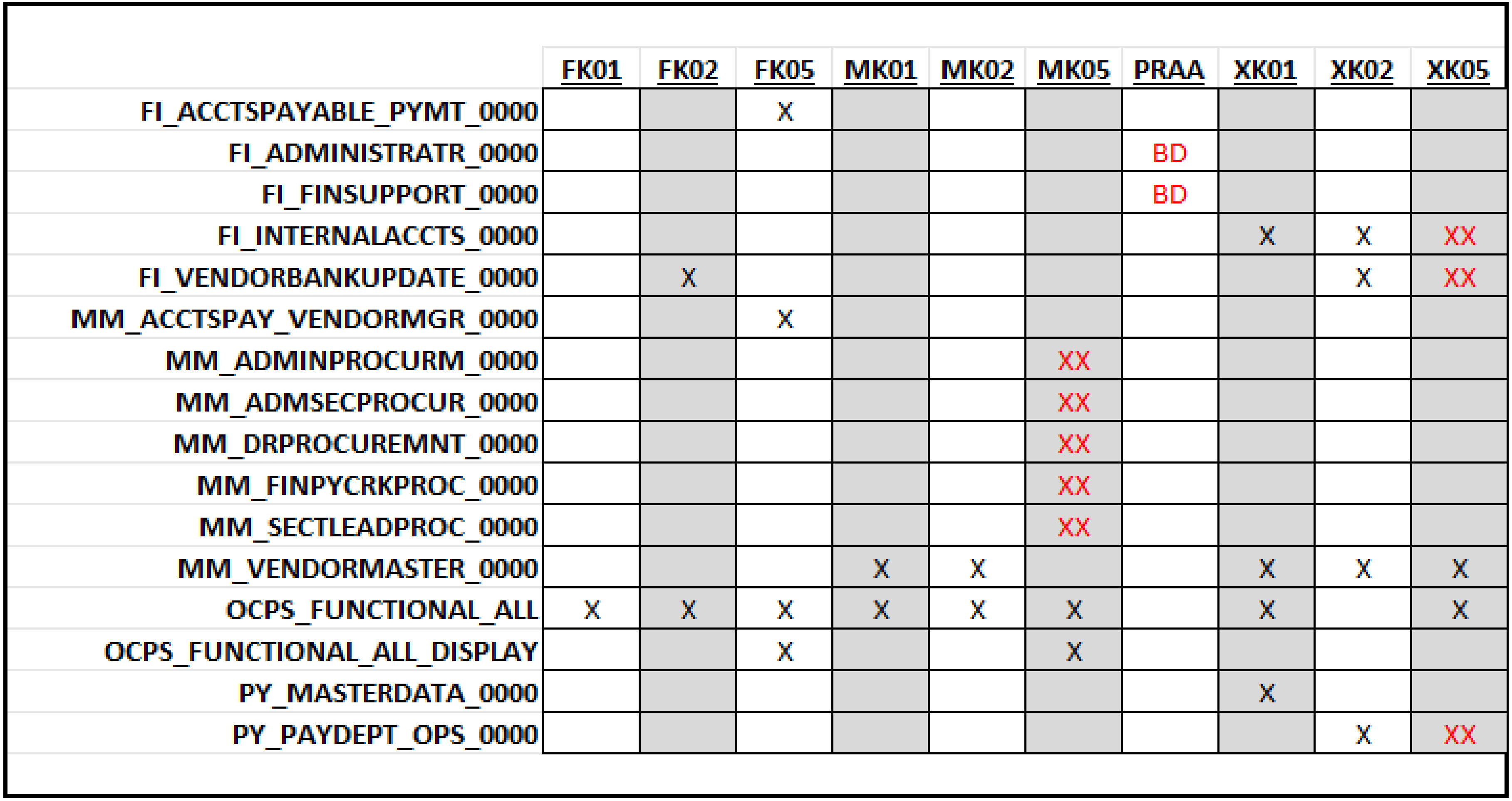
	Accounts Payable	Chief Communications Office	Chief Facilities Office	Chief Financial Office	Chief Operations Officer	Finance	Human Resources	ITS Applications	ITS Customer Care	ITS Information Security	ITS Infrastructure	Office of Mgmt & Budget	Payroll	Procurement	Risk Management	Transportation Administration
FI_ACCTSPAYABLE_PYMT_0000	X															
FI_ADMINISTRATR_0000				BD		BD						BD				
FI_FINSUPPORT_0000				BD		BD						BD				
FI_INTERNALACCTS_0000						X										
FI_VENDORBANKUPDATE_0000	X					X										
MM_ACCTSPAY_VENDORMGR_0000	X															
MM_ADMINPROCURM_0000														X		
MM_ADMSECPROCUR_0000						XX								X		
MM_DRPROCUREMNT_0000														X		
MM_FINPYCRKPROC_0000		X		X		X						X				X
MM_SECTLEADPROC_0000														X		
MM_VENDORMASTER_0000														X		
OCPS_FUNCTIONAL_ALL_DISPLAY			X		X	X	X	X	X	X	X	X		X	X	
PY_MASTERDATA_0000													X			
PY_PAYDEPT_OPS_0000													X			

Note: Red "XX" denotes inadequate control over VMF. Red "BD" denotes inadequate control over Bank Details data in VMF via the PRAA screen.

Source: Information supplied by Information Security on 06/05/2017 and 08/15/2017.

Prepared by: Internal Audit

Table 5: Roles by SAP Transaction



	FK01	FK02	FK05	MK01	MK02	MK05	PRAA	XK01	XK02	XK05
FI_ACCTSPAYABLE_PYMT_0000			X							
FI_ADMINISTRATR_0000							BD			
FI_FINSUPPORT_0000							BD			
FI_INTERNALACCTS_0000								X	X	XX
FI_VENDORBANKUPDATE_0000		X							X	XX
MM_ACCTSPAY_VENDORMGR_0000			X							
MM_ADMINPROCURM_0000						XX				
MM_ADMSECPROCUR_0000						XX				
MM_DRPROCUREMNT_0000						XX				
MM_FINPYCRKPROC_0000						XX				
MM_SECTLEADPROC_0000						XX				
MM_VENDORMASTER_0000				X	X			X	X	X
OCPS_FUNCTIONAL_ALL	X	X	X	X	X	X		X		X
OCPS_FUNCTIONAL_ALL_DISPLAY			X			X				
PY_MASTERDATA_0000								X		
PY_PAYDEPT_OPS_0000									X	XX

Note: Red "XX" denotes that there are individuals in these roles who should not have access to this screen. Red "BD" denotes inadequate control over Bank Details data in the VMF via the PRAA screen.

Source: Information supplied by Information Security on 06/05/2017 and 08/15/2017.

Prepared by: Internal Audit

AUDIT RESPONSE MATRIX FISCAL PERIOD OR AUDIT DATE: 11/28/17_____________

Department / School Name	**Accounts Payable**
Administrator / Department Head	**John Cook/Catherine Nguyen**
Cabinet Official / Area Superintendent	**Dale Kelly**

Exception Noted (Finding / recommendation)	**Management Response (Corrective Action)**	**Responsible Person (Name & Title)**	**Expected Outcome & Completion Date What is the evidence of the corrective action?**
What is? What should be?	**What needs to be done?**	**Who needs to do it?**	**When will the action be completed? (MM/YYYY)**
1. Accounts Payable staff can modify the following information in the VMF: bank details, payment methods, and payment terms, and they process vendor payments. There is not adequate oversight or monitoring of such changes, nor are there adequate compensating controls.	1)Accounts Payable is discussing possible solutions with the District's current financial institution (i.e. Wells Fargo) by leveraging their payment manager service therefore the ability to access/change bank details will not involve personnel that process vendor payments. 2) Alternatively, a new process can be developed which would require a secondary approver of all bank detail changes made. The bank detail will be flagged as critical in the vendor master file, which would require a secondary approver before bank detail changes can be processed	John Cook, Senior Administrator AP	12/2018

2. The VMF Change Log records the details of changes to the bank details field such as who made the change, date and time of change, and whether the person created or deleted data; however, the Change Log does not record the old value or the new value of the field. The only bank details retained in the file are the last ones entered. In this case, an unauthorized change to an incorrect receiving account could be entered, posted and then changed back to the correct account without leaving a record of those changes.	1) Accounts Payable is discussing possible solutions with the District's current financial institution by leveraging their payment manager service and this service would maintain a log record of both old and new bank details. 2) Standard SAP report does not allow for historical bank detail data to be maintained but this field can be flagged as critical which would require secondary approval before payment can be processed.	John Cook, Senior Administrator AP	12/2018
3. No department has acknowledged ownership of the bank details fields in the VMF, so accountability is lacking in that area.	Accounts Payable will discuss with Procurement to determine appropriate of ownership of the bank details field in the VMF.	John Cook, Senior Administrator AP and Procurement	12/2018
4. Analysis and evaluation are needed to correct the PRAA users list and to properly limit access to bank details to only those persons who need it to perform their job responsibilities.	The PRAA users list was removed by ITS from the old roles and new role was created that limits access to required users.	Catherine Nguyen, Senior Director of Finance	11/2017

5. Access to employees' sensitive information should be limited to only by those who have a need. Transaction code PRAA should be modified to prevent access to bank details data fields.	The PRAA users list was removed by ITS from the old roles and new role was created that limits access to required users. The District cannot remove access to the bank details field from transaction code PRAA as it is a required field to create new vendors.	Catherine Nguyen, Senior Director of Finance	11/2017
6. Periodically reviewing and monitoring the VMF Change Log will assist in identifying inappropriate changes or irregularities in sensitive information. There should be a formal written policy and procedure for this monitoring. This will assist in ensuring consistency in practice as well as when training new employees. The Accounts Payable department's focus should be on changes to bank details data fields.	1) Accounts Payable is discussing possible solutions with the District's current financial institution (i.e. Wells Fargo) by leveraging their payment manager service to validate, change and maintain the vendor bank details. If Wells Fargo is selected to perform bank detail changes then the district will obtain their policies and procedures related to this process to ensure that proper controls are in place. On an annual basis, OCPS will review the vendor's SOC report to ensure adherence to their procedures over this process. 2) Policies and Procedures will be developed on a new process which includes a secondary approval of all bank detail changes. The bank detail	John Cook, Senior Administrator AP	12/2018

	will be flagged as critical in the vendor master file, which would require a secondary approver before bank detail changes can be processed.		
7. Access to change a vendor name should be limited. Any changes to the vendor name in the VMF should require approval by an authorized individual.	We have limited access to change a vendor name to required users. Vendor name change should be controlled by Procurement and we will continue to work with Procurement until they assume full responsibility of vendor name changes in the VMF.	John Cook, Senior Administrator AP and Procurement	11/2017
8. A VMF transaction code review process should be established and implemented quarterly by BPSs, users and IT Security.	Access to MK05 and XK05 transactions have been removed from all Finance staff. MK05 and XK05 transactions are owned by Procurement and review of access to these transaction codes should be performed by Procurement as part of their quarterly critical access review to ensure that only authorized users have access to these transaction codes.	Catherine Nguyen, Senior Director of Finance and Procurement	11/2017

AUDIT RESPONSE MATRIX FISCAL PERIOD OR AUDIT DATE: 11/28/17____________

Department / School Name	**Accounts Payable**
Administrator / Department Head	**John Cook/Catherine Nguyen**
Cabinet Official / Area Superintendent	**Dale Kelly**

Exception Noted (Finding / recommendation)	**Management Response (Corrective Action)**	**Responsible Person (Name & Title)**	**Expected Outcome & Completion Date What is the evidence of the corrective action?**
What is? What should be?	**What needs to be done?**	**Who needs to do it?**	**When will the action be completed? (MM/YYYY)**
1. Accounts Payable staff can modify the following information in the VMF: bank details, payment methods, and payment terms, and they process vendor payments. There is not adequate oversight or monitoring of such changes, nor are there adequate compensating controls.	1)Accounts Payable is discussing possible solutions with the District's current financial institution (i.e. Wells Fargo) by leveraging their payment manager service therefore the ability to access/change bank details will not involve personnel that process vendor payments. 2) Alternatively, a new process can be developed which would require a secondary approver of all bank detail changes made. The bank detail will be flagged as critical in the vendor master file, which would require a secondary approver before bank detail changes can be processed	John Cook, Senior Administrator AP	12/2018

2. The VMF Change Log records the details of changes to the bank details field such as who made the change, date and time of change, and whether the person created or deleted data; however, the Change Log does not record the old value or the new value of the field. The only bank details retained in the file are the last ones entered. In this case, an unauthorized change to an incorrect receiving account could be entered, posted and then changed back to the correct account without leaving a record of those changes.	1) Accounts Payable is discussing possible solutions with the District's current financial institution by leveraging their payment manager service and this service would maintain a log record of both old and new bank details. 2) Standard SAP report does not allow for historical bank detail data to be maintained but this field can be flagged as critical which would require secondary approval before payment can be processed.	John Cook, Senior Administrator AP	12/2018
3. No department has acknowledged ownership of the bank details fields in the VMF, so accountability is lacking in that area.	Accounts Payable will discuss with Procurement to determine appropriate of ownership of the bank details field in the VMF.	John Cook, Senior Administrator AP and Procurement	12/2018
4. Analysis and evaluation are needed to correct the PRAA users list and to properly limit access to bank details to only those persons who need it to perform their job responsibilities.	The PRAA users list was removed by ITS from the old roles and new role was created that limits access to required users.	Catherine Nguyen, Senior Director of Finance	11/2017

5. Access to employees' sensitive information should be limited to only by those who have a need. Transaction code PRAA should be modified to prevent access to bank details data fields.	The PRAA users list was removed by ITS from the old roles and new role was created that limits access to required users. The District cannot remove access to the bank details field from transaction code PRAA as it is a required field to create new vendors.	Catherine Nguyen, Senior Director of Finance	11/2017
6. Periodically reviewing and monitoring the VMF Change Log will assist in identifying inappropriate changes or irregularities in sensitive information. There should be a formal written policy and procedure for this monitoring. This will assist in ensuring consistency in practice as well as when training new employees. The Accounts Payable department's focus should be on changes to bank details data fields.	1) Accounts Payable is discussing possible solutions with the District's current financial institution (i.e. Wells Fargo) by leveraging their payment manager service to validate, change and maintain the vendor bank details. If Wells Fargo is selected to perform bank detail changes then the district will obtain their policies and procedures related to this process to ensure that proper controls are in place. On an annual basis, OCPS will review the vendor's SOC report to ensure adherence to their procedures over this process. 2) Policies and Procedures will be developed on a new process which includes a secondary approval of all bank detail changes. The bank detail	John Cook, Senior Administrator AP	12/2018

	will be flagged as critical in the vendor master file, which would require a secondary approver before bank detail changes can be processed.		
7. Access to change a vendor name should be limited. Any changes to the vendor name in the VMF should require approval by an authorized individual.	We have limited access to change a vendor name to required users. Vendor name change should be controlled by Procurement and we will continue to work with Procurement until they assume full responsibility of vendor name changes in the VMF.	John Cook, Senior Administrator AP and Procurement	11/2017
8. A VMF transaction code review process should be established and implemented quarterly by BPSs, users and IT Security.	Access to MK05 and XK05 transactions have been removed from all Finance staff. MK05 and XK05 transactions are owned by Procurement and review of access to these transaction codes should be performed by Procurement as part of their quarterly critical access review to ensure that only authorized users have access to these transaction codes.	Catherine Nguyen, Senior Director of Finance and Procurement	11/2017