Audit Committee

Committee Meeting

~ Agenda ~

300 N New Ballas Rd
Creve Coeur, MO 63141
www.creve-coeur.org/

Tracy Brothers
3144422070

Thursday, August 8, 2019 **9:30 AM** **Administrative Conference Room**

I. Call to Order

Attendee Name	Present	Absent	Late	Arrived
Councilman Robert Hoffman	☐	☐	☐	
Board Member Ronald Abeles	☐	☐	☐	
Vice-Chair Marjorie Richter	☐	☐	☐	
Councilman AJ Wang	☐	☐	☐	
Heather Silverman	☐	☐	☐	

II. Approve Agenda

III. Approve Minutes

Wednesday, December 05, 2018

IV. Old Business

V. New Business

Elect Chair and Vice Chair

FY18 Audit Comments

Pre-Audit Discussion

Fraud Risk Assessment

VI. Adjourment

Audit Committee

Committee Meeting

~ Minutes ~

300 N New Ballas Rd
Creve Coeur, MO 63141
www.creve-coeur.org/

Tracy Brothers
3144422070

Wednesday, December 5, 2018 **10:00 AM** **Administrative Conference Room**

I. Call to Order

Ellen Lawrence	Chairperson
Robert Hoffman	Councilman
Charlotte D'Alfonso	Councilman
Ronald Abeles	Board Member
Marjorie Richter	Vice-Chair
Lori Obermoeller	Director of Finance
Debbie Loso	Assistant
Tracy Brothers	Finance Clerk
Karen Lenk	Auditor

II. Approve Agenda

III. Approve Minutes

Wednesday, August 29, 2018

IV. Old Business

V. New Business

CAFR-Draft

COMMENTS - Current Meeting:

Mrs. Lenk presented the Committee with a draft copy of the CAFR. The Committee and Staff reviewed and discussed the results.

Report on Internal Controls

COMMENTS - Current Meeting:

Ms. Lenk reviewed the internal controls the City currently has in place and their recommendations. Staff commented that with the new software system internal controls and security will be easier to manage.

Report to Audit Committee

Minutes Acceptance: Minutes of Dec 5, 2018 10:00 AM (Approve Minutes)

COMMENTS - Current Meeting:

Mrs. Lenk presented the Committee with the audit report. Mrs. Lenk went through the report and answered questions the committee had. She stated the City is in good financial standing. Mrs. Lenk stated that there will be a new GASB 87 rule concerning leases going into effect 12/31/19. This ruling will effect the audit for FY19.

VI. Adjournment

Motion To: Motion to Adjourn

COMMENTS - Current Meeting:

Meeting adjourned at 10:35 AM.

RESULT:	**ADOPTED [UNANIMOUS]**
MOVER:	Robert Hoffman, Councilman
SECONDER:	Charlotte D'Alfonso, Councilman
AYES:	Lawrence, Hoffman, D'Alfonso, Abeles, Richter

Minutes Acceptance: Minutes of Dec 5, 2018 10:00 AM (Approve Minutes)

CITY OF CREVE COEUR, MISSOURI

REPORT ON INTERNAL CONTROL RELATED MATTERS AND ADVISORY COMMENTS

JUNE 30, 2018

SCHOWALTER & JABOURI, P.C.
Certified Public Accountants & Advisors

The Honorable Mayor, Members
of the City Council and Management
City of Creve Coeur, Missouri

In planning and performing our audit of the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining fund information of the City of Creve Coeur, Missouri (the "City") as of and for the year ended June 30, 2018, in accordance with auditing standards generally accepted in the United States of America, we considered the City's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the City's internal control. Accordingly, we do not express an opinion on the effectiveness of the City's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis.

Our consideration of internal control was for the limited purpose described in the first paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses. Given these limitations during our audit, we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

Our comments concerning internal control and other significant matters are presented as follows:

I. Current Year Matters
II. Status of Prior Year Other Matters

This communication is intended solely for the information and use of management, the Honorable Mayor, the Members of the City Council, and others within the City, and is not intended to be, and should not be used by anyone other than these specified parties.

We will be pleased to further discuss these matters with you and want to express our sincere appreciation to the staff for the cooperation and assistance received during the audit engagement and for the opportunity to serve the City of Creve Coeur, Missouri.

Yours very truly,

Schowalter & Jabouri, P.C.
SCHOWALTER & JABOURI, P.C.

St. Louis, Missouri
December 3, 2018

11878 Gravois Road
St. Louis, Missouri 63127

11777 Gravois Road
St. Louis, Missouri 63127

(314) 849-4999
FAX (314) 849-3486

sjcpa.com

A member of Nexia

I. CURRENT YEAR MATTERS

A. New Accounting Guidance for Leases

In June 2017, the Government Accounting Standards Board (GASB) issued Statement No. 87, *Leases*. GASB 87 is effective for fiscal years beginning January 1, 2020 and is to be applied retroactively. Existing leases are to be recognized and measured based on the facts and circumstances of the lease in the period of implementation of GASB 87, not inception of the lease. Governments generally participate in a significant number of leases and the administration of those leases may be decentralized across the organization, making it difficult to determine exactly which leases may be subject to the new accounting and financial reporting requirements.

We recommend the City begin to evaluate all current leases and contracts to determine if they meet the GASB 87 definition of a lease and develop a plan for the implementation. GFOA has issued a best practice/advisory to assist governments with the implementation.

B. Computer Controls

One of the basic elements of internal control is separation of duties so that no one person controls all phases of an operation. During our audit, we noted the following practices which represent a lack of segregation of duties:

- The Finance Manager is a privileged superuser of the computer application.
- Several individuals have access to the vendor master data file.
- A payroll user access report was not available during our audit.

Management has indicated that the new accounting system implemented in fiscal year 2019 will resolve these segregation of duties concerns. We recommend that the City continue to monitor computer access to the accounting system to ensure proper segregation of duties. At least annually, the supervisor of each department should receive a user access report with all the employees in their department and the access that these employees have.

C. Risk Assessment

The opportunity to commit and conceal fraud exists where there are assets susceptible to misappropriation and inadequate controls to prevent or detect the fraud. Although management addresses risks as they arise in the normal course of everyday business, we recommend that the City perform a risk assessment to identify, analyze, and manage the risk of asset misappropriation. Risk assessment, including fraud risk assessment, is one element of internal control. Thus, ideally, the City's internal control systems should include performance of this assessment.

The risk assessment can be informal and performed by a management-level individual who has extensive knowledge of the City. Ordinarily, the management-level individual would conduct interviews or lead group discussions with personnel who also have an extensive knowledge of the City, its environment, and its processes.

Once areas vulnerable to fraud or other risks have been identified, a review of the City's systems, procedures, and existing controls relating to the identified areas should be conducted. The City should consider the additional controls that need to be implemented to reduce the risk of fraud, considering the nature and extent of controls recommended and the cost of implementing those controls. This assessment of risks and internal controls should be documented to provide the foundation for appropriate communication concerning the City's responsibility for the evaluation and monitoring of the effective operation of controls. Once completed, risk assessments should be reviewed and updated annually or as significant changes occur.

II. STATUS OF PRIOR YEAR OTHER MATTERS

A. Liability Accounts

We recommended the City investigate and take action to resolve liability accounts that appear to be dormant.

Status: Implemented.

B. Risk Assessment

Although management addresses risks as they arise in the normal course of everyday business, we recommended that the City perform a risk assessment to identify, analyze, and manage the risk of asset misappropriation.

Status: See "Other Current Year Matters" for current comment.

C. Computer Controls

We recommended that the City continue to monitor computer access to the GEMS system to ensure proper segregation of duties. At least annually, the supervisor of each department receives a GEMS user access report with all the employees in their department and the access that these employees have.

Status: See "Other Current Year Matters" for current comment.

FRAUD RISK ASSESSMENT
City of Creve Coeur

Fraud, by definition, entails intentional misconduct, designed to evade detection. A fraud risk assessment is a process to identify, analyze, and manage risk. The City must identify both external and internal risks. This assessment process will help management understand how those risks affect their activities, assess their significance, manage their effect and provide for continuous monitoring.

A detailed fraud assessment will be performed by a risk assessment team, which includes the Director of Finance and the Finance Manager who are both familiar with the financial reporting process and internal controls. The City Administrator will also participate in the assessment, as he/she is ultimately accountable for the effectiveness of the City's fraud risk management efforts. This assessment will be performed at least biennially and will be shared with the audit committee. Functions and services that will be included in this assessment are Finance (including Accounting, Purchasing and Payroll), Human Resources Management, and Information Technology.

An effective fraud risk management assessment should identify where fraud may occur and who the perpetrators might be. Therefore, control activities should always consider both the fraud scheme and the individuals within and outside the organization who could be the perpetrators of each scheme. If the scheme is collusive, preventive controls should be augmented by detective controls, as collusion negates the control effectiveness of segregation of duties.

A fraud risk assessment includes three key elements:

- Fraud Risk Identification — Gather information to obtain the population of fraud risks that could apply to the City. Included in this process is the explicit consideration of all types of fraud schemes and scenarios; incentives, pressures, and opportunities to commit fraud; and IT fraud risks specific to the City.
- Assessment of likelihood and significance of identified fraud risk — Assess the relative likelihood and potential significance of identified fraud risks based on historical information, known fraud schemes, and interviews with staff, including the City Council and management.
- Respond to likely and significant fraud risks — Decide what the response should be to address the identified risks and perform a cost-benefit analysis of fraud risks over which the City wants to implement controls or specific fraud detection procedures.

The City will use a grid to document the fraud risk assessment. A blank form of this grid can be found in Appendix A and an example of this grid can be found in Appendix B. The grid example in Appendix B illustrates how the elements of fraud risk identification, assessment, and response are applied in a rational, structured approach. This example begins with a list of identified fraud risks and schemes, which are then assessed for relative likelihood and significance of occurrence. Next, the risks and schemes are mapped to the people and/or departments that may be impacted and to relevant controls, which are evaluated for design effectiveness and tested to validate operating effectiveness. Lastly, residual risks are identified, and a fraud risk response is developed.

FRAUD RISK IDENTIFICATION

The risk assessment team will go through a brainstorming activity to identify the City's fraud risks. Brainstorming enables discussions of the incentives, pressures, and opportunities to commit fraud; risks of

management override of controls; and the population of fraud risks relevant to the City. Other risks, such as regulatory and legal misconduct risk, as well as the impact of IT on fraud risks will also be considered in the fraud risk identification process.

Incentives, Pressures, and Opportunities

Motives for committing fraud are numerous and diverse. The fraud risk identification process will include an assessment of the incentives, pressures, and opportunities to commit fraud.

Opportunities to commit fraud exist throughout the City. These opportunities are greatest in areas with weak internal controls and a lack of segregation of duties. However, some frauds, especially those committed by management, may be difficult to detect because management can often override the controls. Such opportunities are why appropriate monitoring of senior management by the audit committee, supported by external auditors, is critical to fraud risk management.

Risk of Management's Override of Controls

As part of the risk identification process, it is important to consider the potential for management override of controls established to prevent or detect fraud. Personnel within the City generally know the controls and standard operating procedures that are in place to prevent fraud. It is reasonable to assume that individuals who are intent on committing fraud will use their knowledge of the City's controls to do it in a manner that will conceal their actions. It is also important to keep the risk of management's override of controls in mind when evaluating the effectiveness of controls; an anti-fraud control is not effective if it can be overridden easily.

Population of Fraud Risks

The fraud risk identification process requires an understanding of fraud risks and the subset of risks specific to the City. This involves understanding the City's business processes and gathering information about potential fraud from internal sources by interviewing personnel and brainstorming with them and performing analytical procedures.

There are three general categories of fraud risk: fraudulent statements, misappropriation of assets, and corruption. Potential fraud risks to consider in the three general categories include:

1) Intentional manipulation of financial statements, which can lead to:
   a. Inappropriately reported revenues.
   b. Inappropriately reported expenditures
   c. Inappropriately reflected balance sheet amounts, including reserves.
   d. Inappropriately improved and/or masked disclosures
   e. Concealing misappropriation of assets.
   f. Concealing unauthorized receipts and expenditures.

2) Misappropriation of:
   a. Assets by:
      i) Employees.
      ii) Vendors.
      iii) Former employees and others outside the organization.

3) Corruption including:
   a. Bribery and gratuities
   b. Aiding and abetting fraud by other parties (e.g., vendors).
   c. Conflicts of interest
   d. Embezzlement

Fraudulent Financial Reporting

Each of the three general categories includes at least one scheme of how the fraud could occur. For instance, the improper recognition of expenditures can be achieved via numerous schemes, including holding bills to pay in the next fiscal year and improper coding to appropriation lines. Any scheme that is relevant to the City will be considered in the assessment.

The City will use the grid in Appendix A to identify specific areas of greatest risk and as a foundation for customizing the assessment process.

The types of fraudulent financial reporting that would be most probable for a City would be to understate expenditures or miscode expenditures to avoid over spending of appropriations. Conversely, some City's may overstate expenditures to use up appropriation authority. Any intentional misstatement of accounting information represents fraudulent financial reporting.

Another consideration involves fraud where the objective is not to improve the City's financial statements, but to cover up the misappropriation or misuse of assets. In this case, the fraud also includes fraudulent financial reporting.

Misappropriation of Assets

A City's assets can be misappropriated by employees, customers, or vendors. The City will ensure that controls are in place to protect such assets. Considerations to be made in the fraud risk assessment process include gaining an understanding of what assets are subject to misappropriation, the locations where the assets are maintained, and which personnel have control over or access to assets. Common schemes include misappropriation by:

- Employees
  - Creation of, and payments to, fictitious vendors.
  - Charging personal expenses on procurement cards
  - Payment of inflated or fictitious invoices.
  - Invoices for goods not received or services not performed.
  - Theft of inventory
- Employees in collusion with vendors, customers, or third parties.
  - Payment of inflated or fictitious invoices.
  - Invoices for goods not received or services not performed.
- Vendors.
  - Inflated or fictitious invoices.
  - Short shipments or substitution of lower quality goods.
  - Invoices for goods not received or services not performed.

Protecting against these risks requires not only physical safeguarding controls, but also periodic detective controls such as physical counts of inventory.

Corruption

Corruption is operationally defined as the misuse of entrusted power for private gain. There are various types of corruption, and could include such things as taking bribes to award contract, embezzlement, and aiding and abetting vendors to commit fraud.

Information Technology and Fraud Risk

Cities rely on IT to conduct business, communicate, and process financial information. A poorly designed or inadequately controlled IT environment can expose a city to fraud. Today's computer systems, linked by national and global networks, face an ongoing threat of cyber fraud and a variety of threats that can result in significant financial and information losses. IT is an important component of any risk assessment, especially when considering fraud risks. IT risks include threats to data integrity, threats from hackers to system security, and theft of financial and sensitive information. Whether in the form of hacking, of data, viruses, or unauthorized access to data, IT fraud risks can affect everyone. In fact, IT can be used by people intent on committing fraud in any of the three general fraud risk areas. Examples of those risks by area include:

Fraudulent financial reporting

- *Unauthorized access to accounting applications* — Personnel with inappropriate access to the general ledger, subsystems, or the financial reporting tool can post fraudulent entries.
- *Override of system controls* — General computer controls include restricted system access, restricted application access, and program change controls. IT personnel may be able to access restricted data or adjust records fraudulently.

Misappropriation of assets

- *Theft of assets* — Individuals who have access to assets (e.g., cash, inventory, and fixed assets) and to the accounting systems that track and record activity related to those assets can use IT to conceal their theft of assets. For example, an individual may establish a fictitious vendor in the vendor master file to facilitate the payment of false invoices, or someone may steal inventory and record the assets as disposed of, thus removing the asset from the balance sheet.

Corruption

- *Misuse of customer data* — Personnel within or outside the organization can obtain employee data and use such information to obtain credit or for other fraudulent purposes.

Cyber fraudsters do not even have to leave their homes to commit fraud, as they can route communications through local phone companies, long-distance carriers, Internet service providers, and wireless and satellite networks. What is important is that any information — not just financial — is at risk, and the stakes are very high and rising as technology continues to evolve.

To manage the ever-growing risks of operating in the information age, a City should know its vulnerabilities and be able to mitigate risk in a cost-effective manner. Therefore, IT risk has been incorporated into the City's overall fraud risk assessment.

ASSESSMENT OF THE LIKELIHOOD AND SIGNIFICANCE OF IDENTIFIED FRAUD RISKS

Assessing the likelihood and significance of identified risks allows the City to manage its fraud risks and apply preventive and detective procedures rationally. The City must first consider fraud risks on an inherent basis, or without consideration of known controls. By taking this approach, the risk assessment team will be better able to consider all relevant fraud risks and design controls to address the risks. After mapping fraud risks to relevant controls, certain residual risks will remain, including the risk of management's override of established controls.

The risk assessment team must evaluate the potential significance of those residual risks and decide on the nature and extent of the fraud preventive and detective controls and procedures to address such risks.

Likelihood — Team's assessment of the likelihood of a fraud risk occurring is informed by instances of that particular fraud occurring in the past at the City, the prevalence of the fraud risk in the City's industry, and other factors, including the number of individual transactions, the complexity of the risk, and the number of people involved in reviewing or approving the process. The City can have as many categories of the likelihood of potential frauds occurring as deemed reasonable, but three categories are generally adequate: remote, reasonably possible, and probable.

Significance — Team's assessment of the significance of a fraud risk should include not only financial statement and monetary significance, but also significance to criminal, civil, and regulatory liability. Cities can also categorize the significance of potential frauds in as many buckets as deemed reasonable, but three categories are generally adequate: immaterial, more than significant and material.

People/department — As part of the risk assessment process, the City will have evaluated the incentives and opportunities for individuals and departments and should use the information gained in that process to assess which individuals or departments are most likely to have the opportunity to commit a fraudulent act, and, if so, via what means. This information can be summarized into the fraud risk assessment grid and can help the City design appropriate risk responses, if necessary.

RESPONSE TO LIKELY AND SIGNIFICANT FRAUD RISKS

Management will implement a level of control based on the risk tolerance it deems is necessary for the City. While there are thousands of potential controls that could be put in place, the goal is a targeted, structured and efficient approach that delivers the most benefit for the cost of resources. The overall objective is to have the benefit of the control exceed the costs. There may be certain fraud risks that the City considers too expensive and time-consuming to address via controls. However, if a fraud is discovered, zero tolerance for fraud will be applied.

APPENDIX A – BLANK FRAUD RISK ASSESSMENT FORM

Identified Fraud risks and Schemes[1]	Likelihood[2]	Significance[3]	People and/or Department[4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
FINANCIAL REPORTING:							
MISAPPROPRIATION OF ASSETS:							
CORRUPTION:							

1. Identified Fraud Risks and Schemes: This column should include a full list of the potential fraud risks and schemes that may face the City. This list should be formed by discussions with employees and management and brainstorming sessions.
2. Likelihood of Occurrence: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the City establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.
3. Significance to the City: Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to a City. For example, certain fraud risks may only pose an immaterial direct financial risk to the City, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the City. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.
4. People and/or Department Subject to the Risk: As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the City are subject to the risk. This knowledge will assist the City in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.
5. Existing Anti-fraud Internal Controls: Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the City to assess identified fraud risks on an inherent basis, without consideration of internal controls.
6. Assessment of Internal Controls Effectiveness: The City should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Cities should consider and review what monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.
7. Residual Risks: After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including (a) properly designed controls are not in place to address certain fraud risks or (b) controls identified are not operating effectively. These residual risks should be evaluated by the City in the development of the fraud risk response.
8. Fraud Risk Response: Residual risks should be evaluated by the City and fraud risk responses should address such remaining risk. The fraud risk response could be implementing additional controls and/or designing proactive fraud auditing techniques.

APPENDIX B - FRAUD RISK ASSESSMENT FORM
EXAMPLE

The following is a brief example of a fraud risk assessment. This example does not list all possible fraud risks that a city might have. This assessment needs to be done for the following areas: Finance, Human Resources and Information Technology.

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
FINANCIAL REPORTING:							
Revenue Recognition							
Recording receipts in incorrect periods	Remote	Insignificant	Accounting	Manager year end review of receipts.	Tested by Independent staff.	Risk of Management Override.	No further actic receipts are minimal and no benefit to agenc of management record in error.
Expenditure Recognition							
Holding bills	Reasonably possible	Material	Accounting	Input of bills and approval are segregated.	Tested by Independent staff.	Risk of Override.	Independent sta tests year end expenses.
Improper coding of bills	Reasonably possible	Material	Accounting	1) Input of bills and approval are segregated. 2) Review of itemized reports by Senior Management.	1) Tested by Independent staff. 2) Tested by Independent staff.	1) Risk of Override. 2) Adequately mitigated by controls.	1) Independent staff tests vouchers. 2) N/A

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
Misclassification of Balances							
Reporting more receivables and less cash	Remote	Significant	Accounting	Receivable and receipt recording are segregated.	Tested by Management.	Adequately mitigated by controls.	N/A
MISAPPROPRIATION OF ASSETS:							
Cash/Checks							
At time of receipt	Probable	Insignificant	Receptionist	Independent reconciliation of receipts to deposits.	Tested by Management.	Possible that receipts aren't listed on receipt list so there would be nothing to reconcile. However, receive minimal amounts of cash/checks. Any large amounts to be coming in, either have been billed to others or management is awaiting the receipt.	N/A--Receipts are minimal.
Accounts Payable/Expenditures							
Unauthorized Pcard transactions	Probable	Material	Pcard Holders Vendors	1) Pcard Administrator is not a Pcard Holder.	1) Tested by Management.	1) Adequately mitigated by controls.	1) N/A

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
				2) Pcard Administrator checks Pcard charges on-line once or twice a week.	2) Tested by Management.	2) Improper charges would be found after the fact, but policies are in place for disciplinary action for fraudulently acts.	2) There are daily and monthly spend limits so with the controls, any unauthorized amounts would be found by Pcard administrator before the amount would be significant. Also, code of conduct and Pcard policies provide for disciplinary action.
				3) Invoices required for all charges, reviewed by Senior Management, input by staff, approved by Fiscal Officer.	3) Tested by Independent staff.	3) Adequately mitigated by controls.	3) N/A
				4) Pcard Holder can check their charges on-line at any time to check for erroneous charges.	4) Tested by Management.	4) Adequately mitigated by controls-Pcard will issue credits for unauthorized charges.	4) N/A

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
Fictitious Vendors	Remote	Material	Accounting	1) Only Account Associate can set up vendors. 2) Management approval of invoices and review of itemized reports.	1) Tested by Management. 2) Tested by Independent staff.	1) Accounting staff could request a vendor to be set up for a one-time only payment and Account Associate would do so if payment is under $600. Staff could set up a regular vendor, but have IRS and other forms to complete to set this up. 2) Adequately mitigated by controls.	1) One-time vendor amounts are insignificant so no further controls required on that. For other regular vendor set up, any payments would be reviewed by management, who should know most vendors they are dealing with. 2) N/A
Inflated invoices submitted by vendor	Remote	Material	Vendors	Shipments counted upon receipt.	Tested by Management	Adequately mitigated by controls.	N/A
Payroll							
Unauthorized payroll adjustments	Reasonably Possible	Material	Payroll	Management approves monthly and supplemental payroll registers and one-time payment queries.	Tested by Management.	Adequately mitigated by controls.	N/A

Identified Fraud risks and Schemes[1]	Likelihood [2]	Significance [3]	People and/or Department [4]	Existing Anti-fraud Controls[5]	Controls Effectiveness Assessment[6]	Residual Risks[7]	Fraud Risk Response[8]
Capital Assets and Inventory							
Theft by employees	Reasonably Possible	Insignificant	All employees	1) Majority of capital assets are highly visible, needed for daily work, difficult to move and would be noticed if missing. 2) Accounting for assets and inventory taking are segregated.	1) Tested by Management. 2) Tested by Management	1) Slight risk of portable items, such as laptops being taken. However, have only 6 laptops and one person assigned custody of them. 2) Adequately mitigated by controls.	1) N/A--Value of portable items is insignificant and custodian would notice missing laptops. 2) N/A
Theft by others	Remote	Insignificant	Visitors	Portable items, such as laptops are kept in a room that outsiders don't have easy access to.	Tested by Management	Adequately mitigated by controls	N/A
CORRUPTION:							
Kickbacks/conflict of interest							
Contracts improperly awarded	Remote	Material	Accounting	Senior Management reviews all payments before payment and reviews monthly itemized reports	Tested by Independent staff	Risk of Override	Testing by Independent staff

1. Identified Fraud Risks and Schemes: This column should include a full list of the potential fraud risks and schemes that may face the City. This list should be formed by discussions with employees and management and brainstorming sessions.
2. Likelihood of Occurrence: To design an efficient fraud risk management program, it is important to assess the likelihood of the identified fraud risks so that the City establishes proper anti-fraud controls for the risks that are deemed most likely. For purposes of the assessment, it should be adequate to evaluate the likelihood of risks as remote, reasonably possible, and probable.
3. Significance to the City: Quantitative and qualitative factors should be considered when assessing the significance of fraud risks to a City. For example, certain fraud risks may only pose an immaterial direct financial risk to the City, but could greatly impact its reputation, and therefore, would be deemed to be a more significant risk to the City. For purposes of the assessment, it should be adequate to evaluate the significance of risks as immaterial, significant, and material.
4. People and/or Department Subject to the Risk: As fraud risks are identified and assessed, it is important to evaluate which people inside and outside the City are subject to the risk. This knowledge will assist the City in tailoring its fraud risk response, including establishing appropriate segregation of duties, proper review and approval chains of authority, and proactive fraud auditing procedures.
5. Existing Anti-fraud Internal Controls: Map pre-existing controls to the relevant fraud risks identified. Note that this occurs after fraud risks are identified and assessed for likelihood and significance. By progressing in this order, this framework intends for the City to assess identified fraud risks on an inherent basis, without consideration of internal controls.
6. Assessment of Internal Controls Effectiveness: The City should have a process in place to evaluate whether the identified controls are operating effectively and mitigating fraud risks as intended. Cities should consider and review what monitoring procedures would be appropriate to implement to gain assurance that their internal control structure is operating as intended.
7. Residual Risks: After consideration of the internal control structure, it may be determined that certain fraud risks may not be mitigated adequately due to several factors, including (a) properly designed controls are not in place to address certain fraud risks or (b) controls identified are not operating effectively. These residual risks should be evaluated by the City in the development of the fraud risk response.
8. Fraud Risk Response: Residual risks should be evaluated by the City and fraud risk responses should address such remaining risk. The fraud risk response could be implementing additional controls and/or designing proactive fraud auditing techniques.