Montgomery County, Maryland

Office of the County Executive

Office of Internal Audit

Procure-to-Pay Fraud Risk Assessment

December 9, 2019

MCIA-20-3

TABLE OF CONTENTS

Background

Montgomery County's Office of Internal Audit (MCIA) conducted countywide risk assessments in 2010 and 2016. While the 2016 approach to the risk assessment was more data driven (using data from a variety of County sources, including previous audit reports and budget documents), both risk assessments were based on high-level data analytics, versus detailed process reviews to assess existing controls and potential risks. Further, while the 2016 risk assessment provided useful information as a basis for developing an audit workplan, repeating the approach used in 2016 for subsequent countywide risk assessments would be of marginal benefit. Therefore, MCIA implemented a more rigorous risk assessment and targeted audit approach. This approach is discussed below, and was specifically followed in the procure-to-pay (P2P) fraud risk assessment (FRA[1]) initiated by MCIA, and discussed in this report.

This report includes an overview of the overall FRA process and a more detailed overview of the P2P FRA process.

Fraud Risk Assessment Methodology – Overview

The P2P operation is one of a number of enterprise operations (including payroll, cash management, Purchase Cards (not part of the P2P FRA), employee reimbursements) for which core business groups (including the Department of Finance, the Office of Procurement, the Office of the County Attorney, the Office of Human Resources, and the Department of Technology Services) have overall responsibilities. These responsibilities include setting policies and designing appropriate internal controls and processes to ensure a sound control environment and effective operations within the context of the County's de-centralized operational environment. In some cases, core business group responsibilities extend to transaction processing.

As an enterprise operation, P2P also involves execution-level responsibilities within individual County departments and offices, as well as the core business groups. Therefore, any assessment of the existing control environment and associated risks for an enterprise operation must acknowledge that the control environment does not end at the core business groups, but extends out into the departments/offices which are executing the operation; in other words, an enterprise-wide control environment.

The methodology being followed in the P2P FRA reflects this focus on assessing the enterprise-wide control environment, by taking a two-step approach to the risk assessment:

- <u>STEP ONE – Assess Risks and Identify Control Gaps</u>: This step involves the following actions:
    - Mapping the P2P operation from end-to-end, focusing on the core business groups (*Identifying Subprocesses*),

[1] The fraud risk assessment is not an investigation designed to identify and document specific instances of fraud within the County; rather, its focus is on assessing the types of scenarios that could be exploited in a fraudulent manner and the associated risk of fraud being committed. Although the term "fraud" is used, the risk assessment being conducted acknowledges the importance of documenting the potential for waste and abuse within the current control environment for the operation.

  - Identifying the risks or scenarios that potentially could be exploited to commit fraud (*Fraud Scenarios and Inherent Risks*)
  - Identifying and overlaying the internal controls on the operation/process (*Control Environment*),
  - Assessing the likely effectiveness of the controls and the resulting residual risks that appear to remain (*Residual Risks*), and
  - Identification of potential gaps in the internal controls (*Gap Identification*).

  The identification of potential residual risks and gaps in the control environment allows the County to focus corrective actions on additional or re-designed controls that need to be implemented to address any high-risk situations. Step One results in a fraud risk and control matrix (RCM) that (a) identifies the relevant subprocesses, controls, and risks (including the likelihood and impact) of fraud being committed; (b) can be updated based on changes in the process/operation or controls implemented; and (c) provides a structured framework for identifying targeted audits that need to be conducted to test the effectiveness of the existing controls (i.e., Step Two).

- <u>STEP TWO – Testing Effectiveness of Existing Controls</u>: Based on the results of the analyses and deliverables from Step One (which include the identification of the fraud risks/scenarios and the internal controls that have been implemented), this Step involves conducting targeted internal control audits that assess (through testing) how sound the control environment actually is by systematically targeting specific departments/offices and examining specific transactions to determine whether the controls are working as designed. The testing conducted during this step would include testing of the control environment within specific departments selected for audit, as well as testing of the controls implemented within the responsible core business group(s). The results of Step Two testing provide a basis for management to determine whether the existing internal controls mitigate risk to an acceptable level and provide assurance of a sound control environment; as well as identifying instances (within the core business groups and/or the departments) where the controls must be strengthened to achieve an acceptable level of risk. The resulting recommendations for corrective actions to strengthen existing controls would then be tracked and monitored by management and MCIA to ensure full and timely implementation.

The following section of this report provides a summary of procedures performed to conduct the assessment for the P2P operation.

P2P Fraud Risk Assessment – Overview

MCIA engaged SC&H Group (SC&H) to conduct a fraud risk assessment of the County's P2P operation, as applicable to Procurement Contracts (subject to Chapter 11B of the County Code and implementing procurement regulations) and contracts exempt from or not subject to the County's procurement regulations ("Agreements"). SC&H was also tasked with developing an RCM. This assessment focused on identifying fraud risks, not the risk of waste and abuse. The following definition of fraud was applied to this assessment: "Fraud is the misrepresentation of a material fact, knowingly or with reckless indifference to the truth, in order to obtain a benefit or payment to which one would normally not be entitled[2]."

This report provides an overview of the assessment methodology followed in identifying and assessing these fraud risks, and developing the RCM. This assessment was not conducted as an assurance audit, therefore it did not include detailed testing of internal controls. Rather, the intent of this assessment is to inform senior management of high-level controls as they pertain to fraud and fraud management within the County's procure-to-pay operation, and to identify residual risk of fraud after existing controls have been considered.

Detailed testing of internal controls and processes will be conducted by MCIA (under Step Two as discussed above) using the results of this assessment and the resulting fraud RCM.

Given the sensitive and confidential nature of residual fraud risks identified as a result of this assessment, the details of the specific residual high-risk fraud scenarios are not provided as part of this report. These details have been shared with the responsible core business offices so that they may develop and take appropriate corrective actions to strengthen the control processes and systems applicable to the risk scenarios.

Methodology

The assessment focused on the County's core business groups and how they manage risk and controls internally and externally through distribution of policies and requirements to departments/offices. Procedures to develop the RCM were conducted in two phases and are summarized below.

1. Phase 1: Develop the fraud risk universe by identifying potential ways that fraud could be perpetrated against the County ("inherent fraud risks")
2. Phase 2: Identify the preventive and detective controls the County has implemented to mitigate fraud risks, and determine how these controls mitigated the inherent risks, and resulted in the net "residual fraud risks"

Interviews

SC&H conducted interviews with the following core business groups and supporting departments to gain an understanding of the procure-to-pay processes, fraud risks, and controls:

1. Office of Procurement ("Procurement")
2. Office of County Attorney, Division of Finance and Procurement
3. Department of Finance, Controller Division:
    a. Accounts Payable (A/P)
    b. Financial Analysis, Audit, and Compliance (FAAC)
    c. General Accounting
4. Office of Management and Budget

[2] The definition of fraud was obtained from the County's Office of the Inspector General's (OIG) website: https://www.montgomerycountymd.gov/OIG/hotline.html

5. Office of the Inspector General
6. Department of Technology Services, Enterprise Resource Planning (ERP) Division

After the risk and control environments within the County's procure-to-pay operation were documented, SC&H met with a sample of departments to understand how the individual departments manage fraud risks. These departments were selected to obtain a cross-section of purchasing types and organizational structures. For example, some departments have centralized divisions that have contracting or fiscal responsibilities for all divisions. Other departments handle all procurement, contracting, and invoice processing activities de-centralized within each division. The results of department interviews were incorporated into the RCM when additional risks or controls were identified.

County Code, Regulations, and Documentation Review

SC&H reviewed the County's procurement and ethics regulations from the Montgomery County Code and Code of Montgomery County Regulations, as well as the administrative procedure applicable to Agreements. Guidance provided by the core business groups, such as manuals, policies, procedures, trainings, forms, and checklists, were also reviewed. Data, such as payment transaction detail from Oracle, and reporting, such as the annual Record of Procurement report, were also evaluated.

RCM Approach and Content

Assessing the likelihood and impact of each potential fraud risk is a subjective process considering the financial significance as well as the significance to the County's operations, reputation, and legal and regulatory compliance requirements. The initial assessment of fraud risk considered the inherent risk of particular fraud scenarios occurring in the absence of internal controls. After fraud risks were identified, internal controls were mapped to the fraud risks and evaluated for their design effectiveness in mitigating the identified fraud risks. Fraud risks that remained unaddressed by appropriate controls comprise the population of residual fraud risks.

The RCM contains the following three sections:

1. Fraud Risk Details: Describes the fraud risk and potential fraud scenarios that could occur in the County's procure-to-pay operation. Each fraud risk is assigned an inherent risk[3] rating, presented as a number from one to three.
2. Control Details: Describes the control that could prevent or detect the occurrence of fraud within the County, the County department that owns the control, and the design effectiveness of the control. Each control[4] is presented as a number from one to four based on its assessed design effectiveness.
3. Residual Risk Details: Includes the net risk score and the residual risk factors.

[3] Inherent risk is the risk before considering any internal controls in place to mitigate such risk.

[4] Controls were evaluated for their design effectiveness based on limited information (e.g. inquiries and documentation) and were not tested to validate their operational effectiveness. Targeted internal control testing will be conducted during Step Two.

a. Net risk score is the calculation of the *inherent risk* x *control effectiveness.*
b. Residual risk reflects remaining risks after assessing internal controls.

Net Risk

The net risk was compiled considering the fraud risk, internal controls, and residual risk documented in the RCM. Net risk rankings are represented in the following table:

Net Risk Formula Result	Net Risk Ranking
1, 2, 3, 4	Low
5, 6, 7, 8	Moderate
9, 10, 11, 12	High

Fraud Risk Response Forms

As a result of the net risk evaluation procedures, seven fraud risks ("gaps") were determined to be critical to the County and should be addressed in the short-term.

A Fraud Risk Response Form (FRRF) was developed for each "High" net risk. The FRRF provides summarized, key risk criteria, originating from the RCM and includes the following:

Fraud Risk Sheet Section	Description of Content
Fraud Risk Description	Defines the fraud risk
Examples	Describes how the specific fraud risk could be perpetrated in the County's current control environment
Purchasing or Agreement Type	Defines the type of procurement or agreement if the fraud risk only applies to certain types
Net Risk	Contains the final net risk value; low, moderate, or high
Controls	Contains a cross-reference to the controls identified, which were provided as an appendix to the FRRF.
Fraud Schemes	Identifies the fraud schemes related to the fraud risk
Residual Risks	Provides examples of the remaining risks to the County that exist after the consideration of existing controls
Risk Response	Provides potential opportunities to mitigate the risks included in the response section. The County can choose to accept the risk or develop a plan to mitigate the risk
Responsible Department	Defines the department/s who will be assigned ownership of the mitigation plan for the fraud risk

Reporting Meetings

SC&H conducted multiple meetings with leadership representatives from the core business groups and supporting groups to present results for high-risk areas. The purpose of these meetings was to ensure clear understanding of the applicable controls and residual risks; and to determine the departments with responsibilities (lead and major supporting) for developing and implementing corrective action plans to strengthen the applicable controls and processes/systems to mitigate the risks.

SC&H also presented results to the County's Risk Governance Committee on November 29, 2019. The presentation focused on summarizing the assessment's approach and findings, and next steps.

Next Steps

MCIA will monitor progress of responsible departments/offices in developing corrective action plans, and fully and timely implementing actions to strengthen the existing control environment for the high-risk areas.

Summary Results

Montgomery County's P2P operation includes the oversight, guidance, internal controls, and transaction processing from core business groups; and the internal controls and processes executed by departments/offices. Further, the operation includes a variety of agreement types (e.g. those subject to County procurement regulations and those exempt from County procurement regulations) and transaction types (e.g. subject to Authorized Payment Policy and exempt from Authorized Payment Policy). These variables result in complexities to the enterprise-wide P2P control environment as there are multiple scenarios within each fraud risk to consider.

Step One of the FRA focused on inherent fraud risks and the presence of internal controls to mitigate those risks in the P2P operation. The presence of multiple controls was identified in Step One that appear to be designed to mitigate inherent fraud risks within the P2P operation, and in some instances, multiple controls were identified to mitigate a single risk. This assessment of internal controls was based on limited procedures to determine if controls existed and did not confirm control design or operational effectiveness.

While the County has a complex P2P operation, there does appear to be an established control environment with preventive and detective control activities designed to mitigate fraud risks. In addition, the County is working to further enhance its P2P control environment through the implementation of its Risk Governance Committee, FAAC group, and policies and enhanced processes. Further, the County has personnel in the core business groups that are focused on and committed to addressing inherent risks and residual risks.

Through the conduct of the targeted internal control audits planned in Step Two, additional procedures will be performed to evaluate the effectiveness of the P2P control environment, along with identifying any processes where the County should focus its efforts to strengthen and enhance the control environment.