



20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

AUDIT REPORT

CITY AUDITOR

Report Date:	December 8, 2015
Department:	City Attorney
Subject:	Property and Public Liability Fund/Claims Management
Lead Auditor:	Kate Witek

OBJECTIVE

The audit was conducted to determine whether internal controls associated with the Property and Public Liability (PPL) claims management process are in place and operating effectively to ensure compliance with applicable laws and policies and to minimize the risk of undetected errors or fraud.

SCOPE & METHODOLOGY

To accomplish our objective, we:

- Interviewed staff and management to gain an understanding of the Property and Public Liability (PPL) general claims process and the internal control environment.
- Evaluated application level user security and processing controls within the RiskMaster claims management system.
- Performed detailed testing of claim payments processed during the two fiscal years ended June 30, 2015.

BACKGROUND

When Notices of Claim (NOC) against the City are filed in the City Clerk's office, they are immediately forwarded to the City Attorney's office for evaluation and resolution. The litigation division, staffed with 3 attorneys, 2 paralegals, 2 legal assistants, and 1 claims analyst, manages this process, which may or may not end with settlement or litigation.

The City of Mesa is self-insured for the first \$3M in costs for any incident that results in a liability settlement, and purchases excess liability insurance for costs exceeding this threshold. The City also purchases property insurance to protect an estimated \$1B in assets. This policy has a \$50K deductible (\$25K for vehicles), and a limit of \$300M per occurrence. The costs for these policies, as well as all settlements and costs to defend the City against claims and lawsuits, are paid by the PPL Trust Fund.

The PPL fund has a FY 2016 budget of \$5.5M. Unpaid future claims are actuarially estimated and reported annually in the City of Mesa Comprehensive Financial Report. Additional oversight is provided by the City's Self-Insurance Trust Fund Board, which makes recommendations to the City Council pertaining to the financial viability of the trust fund.

CONCLUSION

In our opinion, internal controls associated with PPL claims management are adequate to provide reasonable assurance that the process is managed in accordance with applicable policies, laws and standards. In addition, payment processing controls, including the system interface process between RiskMaster and Advantage (financial system), are sufficient to ensure claims transactions are complete and accurate. However, we noted a few areas in which additional controls could be implemented to further reduce the risk of undetected errors or fraud. Our observations and recommendations are summarized below. For additional details and responses from management, please see the attached Corrective Action Plans (CAPs).

OBSERVATIONS & RECOMMENDATIONS

1. Policies and Procedures

Detailed written policies and procedures are in place, but have not been updated annually as required by department policy. We are recommending that these documents be updated to reflect current practices, expectations, and organizational changes.

2. Segregation of Duties

The City Attorney has established written procedures that include segregation of duties, a standard internal control for reducing fraud risk. For example, multiple individuals are involved in the check issuance process, which reduces the risk of improper payments. In addition, the procedures indicate that the duties of receiving, opening, and closing claims are appropriately segregated from the duties of investigation, settlement, and other claim processing activities. In recent practice, however, the duties of receiving, opening, investigating, settling, and closing claims have primarily been performed by one individual. We are recommending that these duties be segregated as indicated in the department's procedures, and that this segregation be reinforced through RiskMaster security settings.

3. RiskMaster System Security & Administration

The RiskMaster system is used to manage both PPL and Workers' Compensation claims. The system has security settings that allow for a user to be assigned to one or more role-based groups, each of which can be configured to allow or deny the user the ability to perform specific tasks in the system. These settings should be managed by a System Administrator; and changes should be approved by a Data Custodian.

Currently, the RiskMaster System Administrator role (which applies to both the PPL and Workers' Compensation areas of the system) is assigned to 2 employees in the Safety Services/Workers' Compensation office; and there are no officially designated Data

Custodians. In addition, a formal process has not been established for requesting or granting access to the system, or for ensuring users are assigned the most appropriate roles and permissions for their job duties. We are recommending that the City Attorney's Office work with Safety Services and ITD to develop an appropriate process for RiskMaster system administration. This should include designating a separate data custodian for each side of the system, and establishing protocols for managing user roles & permissions.

As a rule, it is a best practice in any sequential record system to "void" (rather than delete) an erroneous or un-needed record. However, if deletions are deemed necessary, it is important to have protocols in place for authorization and documentation. The RiskMaster system has a history tracking feature called "Change Data Capture" (CDC), which tracks the history of all changes to selected fields. It also tracks when records are added, updated, or deleted. However, prior to this audit, the CDC feature was not enabled. We found that a small number of claim files have been deleted from the RiskMaster system, with no explanation and no audit trail. While the number of claims deleted is not significant, the absence of an audit trail is, by definition, an internal control deficiency. We are recommending that protocols be implemented for authorization and documentation of claim deletions, and that the CDC feature be configured to track deletions and other unusual transactions.

CAP#1: Policies and procedures

Observation: Detailed written policies and procedures are in place, but have not been updated annually as required by department policy.

Criteria: According to the City Attorney's Litigation Policies (rev. March 2008):
"The litigation team has a number of policies and procedures that it follows to ensure that the team provides quality legal/litigation services to the City of Mesa and its clients in a proper, professional manner. In order to keep these policies and procedures current and effective, an annual review will be conducted. This review will determine whether the policies and procedures need to be updated, changed or modified. The annual review process is as follows:

1. Review of Current Litigation Policies: *Each year, during the month of November, the Deputy City Attorney will review all of the litigation policies, to determine if any policy needs to be updated.*

The Deputy will meet with the litigation team attorneys to discuss any recommended changes. Thereafter, the Deputy City Attorney, in consultation with the City Attorney, will determine which, if any, changes, modifications and/or additions will be made to the litigation policies and procedures. The decision to adopt any changes or modifications to the litigation policies will be made by the Deputy City Attorney by the end of December.

2. Implementation of Updated Litigation Policies: *The Deputy City Attorney will prepare the updated litigation policies by mid-January. After approval by the City Attorney, the updated litigation policies will be distributed and will go into effect."*

Comments: We agree with the City Attorney that an annual review/update of written policies and procedures is an important process, which helps to ensure that a team provides quality services in a proper, professional manner.

Recommendations: 1-1. Risk management and litigation policies and procedures should be regularly reviewed and updated to incorporate organizational and process changes and to ensure they continue to reflect management's expectations.

**Management
Response:**

1-1. Agree.

Implementation Plan:

The legal assistant to the Litigation Deputy has entered onto the litigation calendar a recurring annual review of the written litigation and claims (risk management) procedures, which will trigger reminders to all litigation attorneys, the RMCA, and the legal assistant to the Deputy.

Individual or Position Responsible:

Legal assistant to the Deputy City Attorney over litigation.

Estimated Completion Date:

Done.

CAP#2: Segregation of Duties

Observation: The duties of receiving, opening, investigating, settling, and closing claims have primarily been performed by one individual.

Criteria: According to the RMCA's written procedures:

"2. Claim Setup

The City Clerk delivers new claims to the City Attorney's Office on a daily basis. These are routed to the Legal Support Assistant (LSA) or Management Assistant (MA) for entry into the claims operating system (Riskmaster). Once entered, the claim files are set up and delivered to the RMCA for investigation and disposition. Claim files are setup by the LSA or MA...."

And:

"8. File Closure

Once a file has been closed through denial or settlement the Riskmaster log notes should be printed and placed in the file on the right hand side. The claim file is then given to the LSA or MA who will close the financials and place the physical file in closed status."

Comments: Segregation of duties is a standard internal control that helps to prevent fraud by ensuring that one employee does not have the ability to execute all phases of a financial process. The underlying basis for this control is that when two or more individuals are involved in a process, fraud is less likely to occur and more difficult to conceal. For example, the current process requires multiple individuals to be involved in the check issuance process, which reduces the risk of improper payments. However, to be most effective, it is also important to examine an entire process and choose the most "incompatible" duties to segregate. Incompatible duties are those which, when combined, are most likely to facilitate a fraud.

According to the procedures cited above, the City Attorney has already segregated incompatible duties within the claims management process, such that one individual should not be able to receive a claim, open the electronic claim file, investigate the claim, negotiate a settlement, and close the electronic claim file. In recent practice, however, the duties of receiving, opening, investigating, settling, and closing claims have primarily been performed by one individual.

Staff in the City Clerk's office reported that they deliver Notices of Claim directly (and only) to the RMCA in the City Attorney's office. The RMCA opens the electronic claim file, investigates the claim, hires consultants, negotiates the settlement, authorizes the payment (up to \$5,000), and closes the claim file. Settlements above \$5,000 must be approved by the Deputy City Attorney. The written procedures cited above, which require the involvement of the LSA or MA, have not been followed.

Recommendations: 2-1. The duties of receiving a claim and opening/closing an electronic claim file should be segregated from the duties of investigating and settling a claim. This segregation should be incorporated into staff assignments and should be reinforced through RiskMaster user security roles and permissions.

**Management
Response:**

2-1. Agree.

Implementation Plan:

1. The claims process has been revised so that notices of claim are sent directly from the City Clerk to the ASA II in the City Attorney's Office. The ASA II opens claims, and ultimately closes them. The Risk Management Claims Analyst does not open or close claims.
2. The RiskMaster System Administrator (currently the Safety Administrator and her MA I) changed security roles and permissions so the RMCA may not open or close claims in RiskMaster. Because of the limited number of people who handle claims for the City, it will be necessary at times to provide temporary claims opening/closing authority to the RMCA, but that must be authorized and documented in emails from the Deputy to the System Administrator.

Individual or Position Responsible:

The City Clerk sends claims directly to the ASA II to be opened. Deputy City Attorney directed Nitra Hawkins to limit claim opening and closing security roles and permissions of the RMCA.

Estimated Completion Date:

Done.

CAP#3: RiskMaster System Security and Administration

- Observations:**
- A formal process has not been established for requesting or granting access to the RiskMaster system; or for ensuring RiskMaster users are assigned the most appropriate roles and permissions for their job duties.
 - The City Attorney's office does not have a designated System Administrator or Data Custodian for the PPL side of the RiskMaster system.
 - Prior to this audit, the RiskMaster system's history tracking feature, which tracks the history of record changes, additions, and deletions, was not enabled.

Criteria: Information technology general control standards for the configuration of application-level security settings dictate that users should only be assigned the access permissions necessary to perform their specific job duties. All requests to add new users and/or make changes to an existing user's access permissions should be approved by a designated Data Custodian. Ideally, the System Administrator and the Data Custodian should not be the same person.

Internal controls should be designed to help ensure the accuracy and completeness of data during processing. According to Government Auditing Standards, an internal control deficiency exists when the design or operation of a control does not allow management to prevent, detect, or correct an impairment, misstatement, or noncompliance. For example, the ability for a system user to delete a record without leaving an audit trail is a significant deficiency, because it allows evidence of irregularities to be destroyed.

As a rule, it is a best practice, particularly in a sequential record system to "void" (rather than delete) an erroneous or un-needed record, because this removes the record from the active population while preserving the data for future reference and audit purposes. However, if deletions are deemed necessary, internal controls should be implemented to ensure deletions are appropriate and authorized; and to preserve an audit trail.

Comments: The RiskMaster system is used to manage both PPL and Workers' Compensation claims. The system has security settings that allow for

a System Administrator to assign users to one or more role-based groups, each of which can be configured to allow or deny the user the ability to perform specific tasks in the system. The current configuration of user roles and permissions in the RiskMaster system does not limit all users to only the access needed to perform their assigned job duties.

Currently, the RiskMaster System Administrator role (which applies to both the PPL and Workers' Compensation areas of the system) is assigned to 2 employees in the Safety Services/Workers' Compensation office; and there are no officially designated Data Custodians.

The RiskMaster system has a history tracking feature called "Change Data Capture" (CDC), which tracks the history of all changes to selected fields. It also tracks when records are added, updated, or deleted. However, prior to this audit, the CDC feature was not enabled. A small number of claim files have been deleted from the RiskMaster system, with no explanation and no audit trail; and, while the number of deleted claims is not significant, the absence of an audit trail is a control deficiency.

- Recommendations:**
- 3-1. The City Attorney's office should work with Safety Services and ITD to develop an appropriate process for RiskMaster system administration. A System Administrator and a Data Custodian should be designated for each side of the system, and protocols should be established for managing user roles & permissions. In addition, a mutually acceptable process for the deletion of claims should be established and documented. The process should include internal controls to ensure deletions are appropriate and authorized; and to ensure that an effective audit trail is preserved.
 - 3-2. RiskMaster system history tracking, i.e. the Change Data Capture feature, should be configured to track changes to claim records, user groups and permissions, deletions, and other unusual activities.

Management Response:

3-1. [Agree.](#)

Implementation Plan:

[The System Administrator currently oversees all of RiskMaster.](#)

The Litigation Deputy serves as the Data Custodian.

The Litigation Unit does not delete claims; nor are any of its staff authorized in Riskmaster to do so. Any extraordinary circumstance that might require deletion could be addressed in RiskMaster by Nitra, but only after the Deputy has authorized the deletion and documented the request.

Individual or Position Responsible:

Deputy City Attorney

Estimated Completion Date:

Done.

3-2. Agree.

Implementation Plan:

The RiskMaster tracking feature is turned "on". Only the System Administrator can change this setting.

Individual or Position Responsible:

The Litigation Deputy City Attorney confirmed with the Safety Administrator that the tracking feature in RiskMaster is "on".

Estimated Completion Date:

Done.