CITY OF DALLAS

Office of the City Auditor

Audit Report

**AUDIT OF CITY OF DALLAS'
SELF-INSURED
GENERAL LIABILITY PROGRAM**
(Report No. A13-007)

April 26, 2013

City Auditor

Craig D. Kinton

Table of Contents

Executive Summary

The Office of Risk Management (ORM) has designed reasonable processes to administer and oversee the Self-Insured General Liability Program (Program). There are opportunities, however, to improve internal controls as follows:

- Secure the password protected user access into the ORM automated claims system. Current practices increase the risk that a user could access the ORM claims system with another user's logon credentials (ID and password) and make unauthorized changes, create false and/or misleading comments within the claims files, or upload fraudulent documents.

> **Background Summary**
>
> The Office of Risk Management administers the City of Dallas' (City) Program. Program claims include automobile, bodily injury, and property damage claims. These claims are generally initiated by individuals who are impacted by incidents caused by City employees on the job.
>
> The City assumed full Program administration responsibilities on May 1, 2012 and discontinued outsourcing claims processing to a Third Party Administrator (TPA). According to City management, establishing and administering the Program's administration internally will provide an estimated $1.1 million savings over a five-year period.
>
> As of the end of Fiscal Year (FY) 2011, *"the City estimates its general liability at $13.3 million, which includes $11.3 million for automobile and general liability and $2 million for probable claims and lawsuits. Of this amount, $4.4 million is estimated to be payable in the next fiscal year."*
>
> **Source**: City of Dallas, Comprehensive Annual Financial Report, FY 2011 and ORM

- Ensure claims processing policies and procedures are consistently followed. A random sample of 30 claims revealed significant percentages of non-compliance with policies and procedures related to: (1) initial claims set-up and handling; (2) investigation and documentation of claims; and, (3) claims settlement and payment.

- Organize files to facilitate monitoring and to protect personal identity information. Audit sampling showed that claim files are not consistently organized and documents containing personal identity information, such as names, social security numbers, driver's license numbers, and medical information, are not securely attached to each file.

We recommend the Director of ORM:

- Require City network and ORM claims system passwords be changed with the assistance of the Director of the Department of Communication and Information Services (CIS) and the claims processing software vendor, TriStar, to immediately resolve the potential security issues

- Ensure employees receive training on the importance of maintaining logon credential security

- Periodically monitor compliance with ORM policies and procedures and document the results

- Develop file organization procedures to facilitate monitoring efficiency and protect personal identity information

The objective of the audit was to determine the adequacy of the design of the processes used to administer and oversee the Program. The audit period covered May 2012 through November 2012. We also reviewed certain related transactions and records before and after that period.

Management's response to this report is included as Appendix III.

Auditor Follow-Up Comments

Management disagreed with Recommendation IV (page 9) to develop file organization procedures to facilitate monitoring efficiency and protect personal identity information. Given the high error rates noted for compliance with policies and procedures related to initial claims set-up and handling (30 percent) and investigating and documenting of claims (80 percent), we encourage management to reconsider its position on organizing files in a consistent manner to facilitate monitoring and protection of personal identity information.

Management's response contained inaccurate statements as follows:

(1) *".…the files audited and found to be in disarray were not within the scope of the audit (as indicated in the Engagement Letter)."*

The Engagement Letter established the audit scope as: *"…policies and procedures for the Program and general liability transactions processed after May 1, 2012; however, certain other matters, procedures, and transactions outside that period may be reviewed to understand and verify information during the audit period."* Twenty of the 30 files sampled were in process after May 1, 2012; therefore, ORM had the responsibility to ensure that the claims had been processed. The ORM still had oversight responsibility for ensuring the remaining ten claim files initiated and closed prior to May 1, 2012 were processed appropriately.

(2) *"….none of the claim files were found to be disorganized."*

None of the 60 files reviewed for this audit were organized in a consistent manner. Many files were either missing documentation or contained duplicate documents.

Audit Results

Overall Conclusions

The Office of Risk Management (ORM) has designed reasonable processes to administer and oversee the Self-Insured General Liability Program (Program). There are opportunities, however, to improve internal controls as follows: (1) secure the password protected user access into the ORM automated claims system; (2) consistently follow ORM policies and procedures for initial claims set-up and handling; investigating and documenting claims; and, claims settlement and payment; and, (3) develop file organization procedures to facilitate monitoring efficiency and protect personal identity information.

Claims System Is Not Adequately Secured

Access to ORM claims system is not adequately secured. An e-mail, sent on May 3, 2012 to the ORM Safety Supervisor, contained the login IDs and passwords for multiple ORM employees, including ORM management. The e-mail was forwarded to ORM Safety Officers on August 3, 2012. Although the e-mail recommended that upon receipt of the e-mail, each ORM Safety Officer should

Password Security
"Keep confidential passwords that are used to access the corporate mainframe or network, or departmental networks. Disclosure is not allowed under any circumstances. Users are advised to create passwords that are not obvious and/or easily guessed by others."
Source: Administrative Directive 2.24: *Computer Security*, Section 5.5.6

login to the system and change their individual passwords, there were no controls to ensure that the password changes were performed timely. All eight Safety Officers did not change their temporary passwords until the auditor performed user access verifications on or subsequent to August 3, 2012.

In addition, an ORM employee indicated via e-mail that, during the employee's absence, another ORM co-worker could access the system using the employee's logon credentials (ID and password). As a result, there is an increased risk that a user could access the ORM claims system with another user's logon credentials and make unauthorized changes, create false and/or misleading comments within the claims files, or upload fraudulent documents.

According to the Federal Information System Controls Audit Manual (FISCAM), Section AC-2.1, the password selection is to be controlled by the assigned user and is not to be subject to disclosure. Additionally, Administrative Directive 2-24, *Computer Security*, Section 5.5.6 references the requirement for secure and confidential passwords on City systems.

Recommendation I

We recommend the Director of ORM, with the assistance of the Director of the Department of Communication and Information Services (CIS) and the claims processing software vendor, TriStar, require City network and ORM claims system passwords be changed immediately to resolve the potential security issues.

Recommendation II

We recommend the Director of ORM ensures that employees receive training on the importance of maintaining logon credential security.

Please see Appendix III for management's response to the recommendations.

Office of Risk Management's Policies and Procedures Are Not Consistently Followed

ORM does not consistently follow their policies and procedures for claims processing. Without consistent adherence to policies and procedures, ORM cannot ensure that claims are processed accurately and timely.

A random sample of 30 claims showed that multiple claims were noncompliant with established ORM policies and procedures as follows:

- **Nine of 30 claims, or 30 percent, were noncompliant with policies and procedures related to initial claims set-up and handling**:

  o Six claims were not assigned within the timeframe required by policies and procedures

  o Two claims were not date stamped and, as a result, the date of receipt could not be determined

  o One claim was missing the Notice of Claim and the incident date could not be determined

  According to Section 1 of the ORM Liability Procedure Manual (Manual), all new claims received are to be date stamped upon receipt. In addition, if the claim is received prior to 2:00 PM, it is to be assigned to an adjuster on the same day. If the claim is received after 2:00 PM, it is to be assigned the next day.

- **Twenty-four of 30 claims, or 80 percent, were noncompliant with policies and procedures related to investigating and documenting claims:**

  o Eleven claims exceeded the allowable time for claimant/attorney contact and/or sending the acknowledgement letter

  o Two claims related to bodily injuries did not contain the required accident/incident scene photos

  o Twenty claims exceeded the allowable time for management review or lacked evidence that a review occurred

  o Eleven claims were not compliant with regard to departmental response time

    o One claim lacked management approval for missing claimant statement

Per Section 3 of the Manual, each claimant/attorney is to be contacted within three working days of receiving the claim, an Acknowledgement Letter must be sent within three working days, and claims resulting in bodily injury should have photos of the accident/incident scene in the file. Per Section 4 of the Manual, Official responses should be sent within two business days to the Safety Supervisor. The Safety Supervisor will be responsible for ensuring that the department answers the damage claim within 15 business days. Per Section 6 of the Manual, initial management review of claims should occur within 30 days from the date of assignment.

- **One of 30 claims, or three percent, was noncompliant with policies and procedures related to claims settlement and payment:**

    o One settled claim was missing the settlement request form

Per Section 13 of the Manual, adjusters are to prepare a request for payment (delivery confirmation form) and submit the form to the Liability Claim Supervisor for approval. This form is to include claim documentation and should be reviewed by two members of management for signature. In addition, all claim settlement checks require an executed release prior to delivery to a claimant.

Recommendation III

We recommend the Director of ORM periodically monitor compliance with ORM policies and procedures and document the results.

Please see Appendix XX for management's response to the recommendation.

Claim Files Are Not Organized to Facilitate Monitoring and to Protect Personal Identity Information

The claim files were not organized to facilitate monitoring and to protect personal identity information. Without standard claim file organization, ORM management cannot efficiently monitor that claims are:

- Processed in accordance with ORM policies and procedures which require:

  o The Claims Supervisor to, at a minimum, perform a review of the claim file within 30 days from the date of assignment

  o Claims Management (Claims Manager and Liability Claims Supervisor) to perform subsequent claim file reviews every 30-45 days until file closure

  o Complete claim file documentation before a claim is finalized

The claims also showed that personal identity information, such as names, social security numbers, driver's license numbers, and medical information is gathered as a routine part of claims processing; however, this information is not adequately secured in each claim file. Securing documents in a claim file reduces the possibility of documents falling out of claim files, being mixed in with other claim files, or lost altogether.

Administrative Directive 2-51: *Records Management*, Section 1, requires ORM *"to create accurate and complete records of all city business transactions, to preserve those records in a manner that ensures they have not been lost, damaged or altered without authorization and documentation, and that the records are destroyed in accordance with state law and City Code."* The Texas Identity Enforcement and Protection Act, Section 48.102 and the Texas Insurance Code, Section 4151.115 require personal identity information be protected from disclosure.

Recommendation IV

We recommend the Director of ORM develop file organization procedures to facilitate monitoring efficiency and protect personal identity information.

Please see Appendix III for management's response to the recommendation.

<div align="right">

Appendix I

</div>

Background, Objective, Scope and Methodology

Background

The Office of Risk Management (ORM) administers the City of Dallas' (City) Self-Insured General Liability Program (Program). Program claims include automobile, bodily injury, and property damage claims. These claims are generally initiated by individuals who are impacted by incidents caused by City employees on the job. As of the end of Fiscal Year (FY) 2011, the City estimated its general liability claims at $13.3 million. This amount included $11.3 million for automobile and general liability claims and $2 million for probable claims and lawsuits with $4.4 million of the total amount estimated to be payable in FY 2012.

On April 11, 2012, Dallas City Council authorized the City to internally administer the Program. This change became effective on May 1, 2012. Before this effective date, the City was under contract with a Third Party Administrator (TPA) that managed the majority of the claims process. The City determined that providing claims administration internally would generate an estimated cost savings of $1.1 million over the next five years.

The ORM has 25 employees with primary responsibilities for the Program, which include a: (1) Director; (2) Assistant Director; (3) Claims Manager; (4) Claims Supervisor; (5) Safety Supervisor; (6) Three General Liability Adjusters; (7) Three Worker's Compensation Coordinators; (8) Two Senior Risk Analysts/Risk Transfer; (9) Eleven Safety Officers; and, (10) One Contractual Transfer Coordinator.

As shown in Chart I on the following page, property damage claims consistently accounted for a significant number of Program claims. For FY 2011, ORM processed a total of 1,301 claims of which 915, or 70 percent, were property damage claims.

Chart I

## General Liability Claims Volume
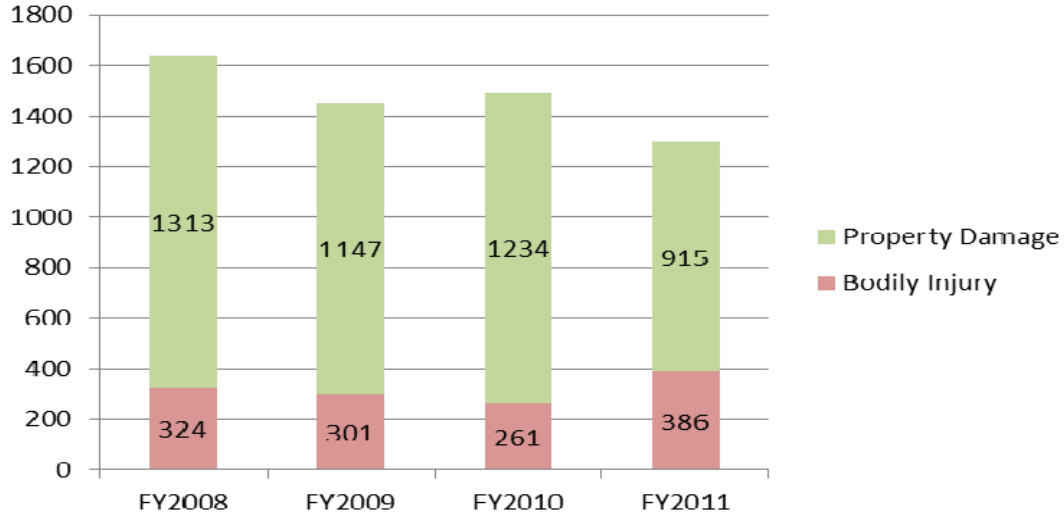
Source: Office of Risk Management's Claim System – cSTAR

As shown on Chart II below, there were 962 claims which were not paid ($0). Claims were not paid due to a: (1) withdrawal of the claim by the claimant; (2) lack of response from the claimant; or, (3) determination that the City was not liable. The City paid 339 claims during FY 2011.

Chart II

Frequency of Liability Claims by Payout Size, FY 2011
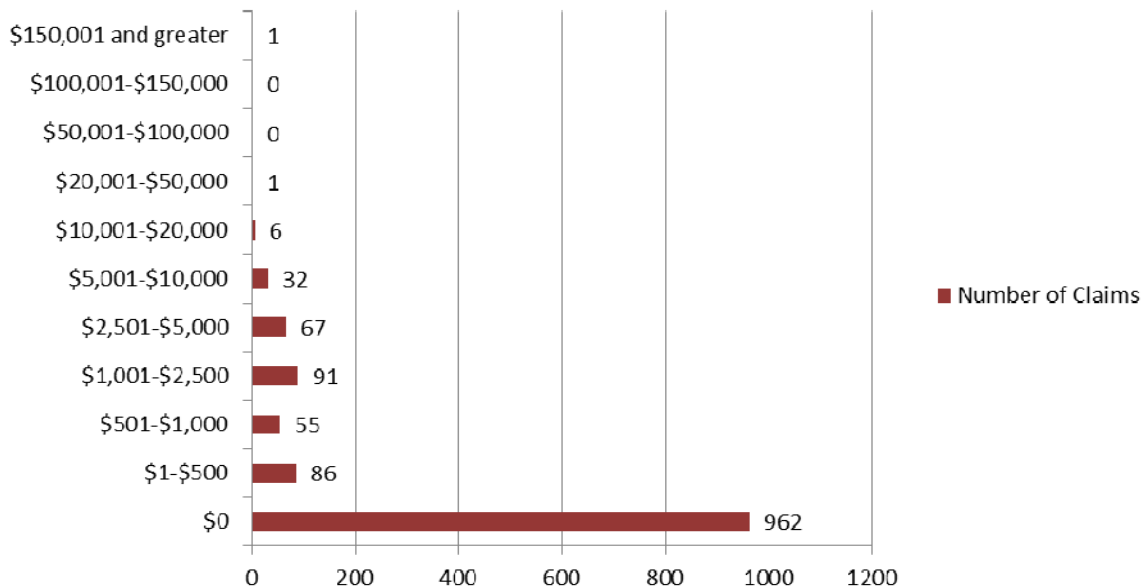
Source: Office of Risk Management's Claim System – cSTAR

Objective, Scope and Methodology

This audit was conducted under authority of the City Charter, Chapter IX, Section 3 and in accordance with the Fiscal Year 2012 Audit Plan approved by the City Council. This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The objective of the audit was to determine the adequacy of the design of the processes used to administer and oversee the Program. The audit scope included claims processed from May 2012 through November 2012; however, certain other matters, procedures and transactions occurring outside that period may have been reviewed to understand and verify the information related to the audit period.

To achieve the audit objective, we performed the following procedures:

- Conducted interviews with ORM management to better understand the general liability claims process

- Researched applicable State and local statutes that impact ORM processes

- Selected and tested a random sample of 30 ORM claims from May 2012 through November 2012

- Reviewed ORM policies and procedures

<div align="right">

Appendix II

</div>

Major Contributors to This Report

Carol Smith, CPA, CIA, CFE, CFF, Audit Manager
Sam Willson, Project Manager
Theresa Hampden, CPA, Quality Control Manager

Appendix III

Management's Response

RECEIVED

APR 1 5 2013

City Auditor's Office

CITY OF DALLAS

Memorandum

DATE: April 15, 2013

TO: Craig D. Kinton, City Auditor

SUBJECT: Response to Audit Report: Audit of City's Self-Insured General Liability Program

Our responses to the audit report recommendations are as follows:

Recommendation I:

We recommend the Director of ORM, with the assistance of the Director of the Department of Communication and Information Services (CIS) and the claims processing software vendor, TriStar, require City network and ORM claims system passwords be changed immediately to resolve the potential security issues.

Management Response / Corrective Action Plan

Agree ☒   Disagree ☐

(The CStar claims software is leased from Tristar Risk Management; therefore, the claims software is completely independent of the City's network and all passwords are assigned and distributed by Tristar.)

As of December 21, 2012:
- TriStar reset each employee's password
- Tristar has programmed all passwords to change every 90 days

Implementation Date
December 21, 2012

Responsible Manager
Juan Azcarate, Claims Manager II

Recommendation II:

We recommend the Director of ORM ensures that employees receive training on the importance of maintaining logon credential security.

"Dallas: The City That Works: Diverse, Vibrant, and Progressive."

Management Response / Corrective Action Plan

Agree ☒   Disagree ☐

As of December 21, 2012,
- ORM employees were briefed on safeguarding of passwords
- Each ORM employee reviewed and signed the City's Computer Security Agreement

Implementation Date
December 21, 2012

Responsible Manager
Juan Azcarate, Claims Manager II

Recommendation III:

We recommend the Director of ORM periodically monitor compliance with ORM policies and procedures and document the results.

Management Response / Corrective Action Plan
Agree ☒   Disagree ☐

A weekly report is generated to show the number of outstanding diaries, department requests for information and check requests. An external audit will be performed annually to monitor compliance of the procedures.

Implementation Date
March 25, 2012

Responsible Manager
Debra Johnson Ojo, Director of Risk Management

Recommendation IV:

We recommend the Director of ORM develop file organization procedures to facilitate monitoring efficiency and protect personal identity information.

Management Response / Corrective Action Plan
Agree ☐   Disagree ☒

During the original audit, the City Auditor's Office audited claim files that were handled by the previous third-party administrator which was not within the scope of the audit (as indicated in the Engagement Letter). As a result of that audit, the files were noted to be unorganized.

ORM notified the City Auditor's Office that the files audited and found to be in disarray were not within the scope of the audit. The City Auditor's Office subsequently audited a different batch of claims within the scope. During the second audit, none of the claim files were found to be disorganized. Therefore, this recommendation is related to the first audit which was outside the scope and considered invalid.

"Dallas: The City That Works: Diverse, Vibrant, and Progressive."

Additionally, the file organization cited in the audit finding was not linked to any deficiencies in the claims handling process. None of the "claims processing" findings resulted from lost, damaged, altered or inappropriately stored documents. Therefore, this recommendation is not applicable to AD 2-51, the Texas Identify Enforcement and Protection Act, Section 48.102 nor the Texas Insurance Code, Section 4151.115.

(For informational purposes, as of January 1, 2013, the claim files were converted to a paperless system.)
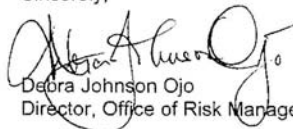
Implementation Date
N/A

Responsible Manager
Juan Azcarate, Claims Manager II

Sincerely,

Debra Johnson Ojo
Director, Office of Risk Management

c: Mary K. Suhm, City Manager

"Dallas: The City That Works: Diverse, Vibrant, and Progressive."