The Auditor of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver’s government. He also chairs the City’s Audit Committee.

The Audit Committee is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City’s finances and operations, including the integrity of the City’s financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

Audit Committee

Dennis Gallagher, Chair  Robert Bishop
Maurice Goodgaine  Jeffrey Hart
Leslie Mitchell  Timothy O’Brien, Vice-Chair
Rudolfo Payan

Audit Staff

Audrey Donovan, Deputy Director, CIA, CGAP, CRMA
Shannon Kuhn, IT Audit Supervisor, CISA
Nicholas Jimroglou, Lead IT Auditor, CISA
Jakki Boline, Senior IT Auditor

You can obtain copies of this report by contacting us at:

Office of the Auditor
201 West Colfax Avenue, Department 705 • Denver CO, 80202
(720) 913-5000 • Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at:

www.denvergov.org/auditor

A2014-012
Mr. Frank Daidone, Chief Information Officer  
Technology Services  
City and County of Denver  

Dear Mr. Daidone:

Attached is the Auditor’s Office Audit Services Division’s report of the audit of Change Management Practices. The purpose of the audit was to assess the effectiveness of change management, and to review internal controls associated with change management used by Technology Services to manage changes to City systems, applications, and networks.

We examined Technology Services’ change management policies and procedures, authorization and approval of changes, testing, change status tracking and reporting, and program library management.

We identified several areas related to information technology governance where controls need to be improved. Our recommendations address improvements to policies and procedures, enhancements to change management processes, increased monitoring of failed changes, and increased security over program libraries.

If you have any questions, please call Kip Memmott, Director of Audit Services, at 720-913-5000.

Sincerely,

Dennis J. Gallagher  
Auditor  

DG/sk  
cc: Honorable Michael Hancock, Mayor  
Honorable Members of City Council  
Members of Audit Committee  
Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer  
Ms. Janice Sinden, Chief of Staff  
Mr. David P. Edinger, Chief Performance Officer  
Ms. Beth Machann, Controller  
Ms. Janna Young, City Council Executive Staff Director  
Mr. Stephen Coury, Chief Information Security Officer  
Mr. L. Michael Henry, Staff Director, Board of Ethics  
Mr. Scott Cardenas, Chief Technology Officer  
Mr. Alena Gouveia, Manager of IT Governance  

To promote open, accountable, efficient and effective government by performing impartial reviews and other audit services that provide objective and useful information to improve decision making by management and the people.  
We will monitor and report on recommendations and progress towards their implementation.
AUDITOR’S REPORT

We have completed an audit of Change Management Practices. The purpose of the audit was to assess the effectiveness of internal controls used by Technology Services to manage changes to application and system software, as well as changes to networks, databases, and hardware.

This performance audit is authorized pursuant to the City and County of Denver Charter, Article V, Part 2, Section 1, General Powers and Duties of Auditor, and 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit showed marked improvements to the change management process since it was implemented in 2013. Technology Services has purchased change management software, established an Information Technology Service Management Team, implemented a change management process based on the Information Technology Infrastructure Library best practice framework, and provided training and support to Technology Services personnel to make this process a success.

While these improvements have helped to strengthen the change management process and control structure, we noted weaknesses in the areas of process maturity and information security. The audit found that the City could make improvements to the change management structure to ensure that the process matures and information security is strengthened. This report contains recommendations that will improve the information technology change control process and ensure that it is effectively and economically managed.

We extend our appreciation to Technology Services and the personnel who assisted and cooperated with us during the audit.

Audit Services Division

Kip Memmott, MA, CGAP, CRMA
Director of Audit Services
Background

Change management is a set of procedures that is used to manage all modifications to hardware and software. Effective change management processes minimize the disruption of information technology services and systems. Without a change management process, unplanned system outages could negatively impact City agencies and citizens.

Purpose

The purpose of this audit was to assess the control structure around introducing changes to the City’s systems and applications production environment. Specifically, we analyzed internal controls over Technology Services’ change management practices, including determining whether: 1) procedures are developed, designed, implemented, monitored, and aligned with best practices; 2) changes are initiated and authorized to meet business needs; 3) changes are appropriately tested and approved prior to being introduced into production; 4) emergency changes are approved and a business justification exists for the expedited change; and 5) program code storage controls allow only authorized, tested changes into production.

Highlights

Our audit showed marked improvements to the change management process since it was implemented in 2013. Technology Services has purchased change management software, established an Information Technology Service Management Team, implemented a change management process based on the Information Technology Infrastructure Library best practice framework, and has provided training and support to Technology Services personnel to make this process a success.

While these improvements have helped to strengthen the change management process and control structure, we noted weaknesses in the areas of process maturity and information security. Specifically:

- Documentation for the change management process should be updated to include suggested items contained in best practice frameworks.
- Performance metrics and third-party service level agreements have not been fully developed.
- Existing controls and processes for emergency changes should be enforced to prevent inappropriately prioritizing emergency change requests and approvals.
- The Configuration Management Database should be utilized and a formal process established to ensure on-going accuracy and completeness of configuration items.
- Password and user access controls over application changes need to be strengthened.
- Procedures need to be established for reviewing and monitoring privileged accounts.

For a complete copy of this report, visit www.denvergov.org/auditor
Or Contact the Auditor’s Office at 720.913.5000
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION &amp; BACKGROUND</td>
<td>1</td>
</tr>
<tr>
<td>SCOPE</td>
<td>3</td>
</tr>
<tr>
<td>OBJECTIVE</td>
<td>3</td>
</tr>
<tr>
<td>METHODOLOGY</td>
<td>4</td>
</tr>
<tr>
<td>FINDING</td>
<td>6</td>
</tr>
<tr>
<td>Technology Services Has Not Fully Mitigated the Inherent Risks within the Change Management Process and Continued Improvements Are Needed To Fully Mature the Process</td>
<td>6</td>
</tr>
<tr>
<td>RECOMMENDATIONS</td>
<td>14</td>
</tr>
<tr>
<td>AGENCY RESPONSE</td>
<td>16</td>
</tr>
</tbody>
</table>
INTRODUCTION & BACKGROUND

The practice of change management in the field of information technology (IT) is analogous to the use of traffic lights on city streets. The purpose of traffic lights is to control the flow of motor vehicle traffic and to help pedestrians safely cross intersections. Similarly, change management is used to control IT system and application changes as they flow through the process sequences, also known as control gates. Without traffic lights, collisions are bound to occur, which would disrupt the flow of traffic. Similarly, if IT changes are introduced with uncontrolled process sequences, disruptions to systems and services are highly likely. In the absence of a change management process, an organization is more likely to experience disruptions to business critical systems and automated services on which customers and citizens rely.

On October 30, 2013, the City and County of Denver implemented a change management process to ensure that changes to IT applications and systems follow a standard process based on the Information Technology Infrastructure Library (ITIL) framework. This best practice ensures that system changes introduced into the production environment are evaluated, tested, and implemented in a controlled manner to reduce risks and improve efficiency. It is important to use a best practice or framework such as ITIL when establishing a new technology process such as change management. The ITIL framework provides proven building blocks necessary to develop and properly structure and streamline steps to achieve efficiency and effectiveness. Other frameworks and standards that address change management include the Federal Information Systems Control Audit Manual (FISCAM) and Control Objectives for Information and Related Technology (COBIT).

Types of Changes To Be Governed through a Change Management Process

There are four categories of IT changes that should go through a change management process: small, routine, comprehensive, and emergency. Small changes are minor, such as an enhancement to the design of an application that might change the look and feel of the application to the end user. Routine changes typically address preventative maintenance, such as the need to apply a patch to fix a known vulnerability within an application or system to help reduce potential downtime or security flaws. The patch released to resolve the recently discovered vulnerability known as Heartbleed is an example of a system patch that should go through the change management process.

Comprehensive changes add new functionally or features to an existing application and result from a business request. Emergency changes address immediate business requirements or urgent security concerns.

Although different types of changes vary by application and system, all changes should follow the change management process established by an organization’s IT management. Typically a requested change is evaluated, prioritized, and coordinated...
with system owners. Next, a developer programs the code in a separate test environment to prevent disruption of production processes. Depending on the system or application, this activity may be handled by a third-party vendor. A series of tests are conducted to determine if the code functions as intended and meets the needs of the business. These stages are referred to as Quality Assurance and User Acceptance Testing. Finally, the requested change is presented to a Change Advisory Board for approval and the code is moved from the test environment into production. This move is performed by someone who did not develop the code. This change in task ownership is known as segregation of duties, and it helps prevent fraud and error by having more than one person perform a task. Without segregation of duties, a developer could implement malicious code into production, or modify the program in such a way that could lead to downtime or errors. Figure 1 shows the path of a change moving through a change management process from initiation to implementation. Unauthorized changes that do not follow the stages of the change management process could result in excessive downtime, corruption of data, and system errors.

**FIGURE 1: STAGES OF A CHANGE MANAGEMENT PROCESS**

Source: Created by Audit Services Division Staff.

**Change Management Risks in the Workplace**

There are risks associated with not having change management procedures in place. Change management risks can encompass minor losses in productivity to multi-million-dollar losses related to dwindling customer confidence, missed revenue opportunities, and lost data. The most serious risk resulting from poor change management is loss of life.

In 2012, Knight Capital Group, Incorporated, reported a quarterly loss of $389.9 million from a significant software error that nearly pushed it into bankruptcy. Improperly installed software malfunctioned and increased trading, causing volume to surge and prices to swing in dozens of securities that day.¹ Thorough change testing may have prevented this catastrophic event. Another example took place in 2004 when a highly complex IT system was introduced in the United Kingdom’s Child Support Agency. At the exact same time, the Department for Work and Pensions decided to restructure the entire agency. The Child Support Agency’s and Department for Work and Pensions' software systems were completely incompatible, and irreversible errors were introduced as a result. The Child Support Agency’s system overpaid 1.9 million people and

---

underpaid another 700,000 people, there were $7 billion in uncollected child support payments and a backlog of 239,000 cases, and 36,000 new cases became “stuck” in the system. These errors have cost the British taxpayers more than $1 billion to date.\textsuperscript{2, 3}

Tragically, the most serious risks involve loss of life. The \textit{American Journal of Public Health} reported on a software-related mishap that resulted in death. In 2001, excessive radiation doses were dispensed due to faulty use of software, killing five Panamanian cancer patients.\textsuperscript{4} While many City agencies’ business applications do not pose a risk of death in the event of a malfunction, there are some applications that could contribute to dire consequences for citizens, such as 911 Computer Aided Dispatch.

\section*{Change Management Tools}

To facilitate the change management process, the City uses software tools to initiate, track, and monitor changes throughout the change lifecycle. These software tools enforce the required chain of events to prevent the change management process from being circumvented. The City implemented change management software in October 2013, which is used as a workflow and approval tool to control changes to City applications and systems. Several software utility packages are also used to provide developers with requirements, version control, and issue tracking during the development process. Additionally, a network utility program, which monitors changes to network components and firewalls, detects and reports changes. A separate content management tool assists web developers in modifying City websites.

\section*{SCOPE}

The scope of the audit was limited to internal controls over Technology Services’ change management practices for existing application systems used in production processing. The audit period addressed all changes since October 30, 2013, which is when the new change management process was established.

\section*{OBJECTIVE}

The objective of this audit was to assess the efficiency and effectiveness of change management processes used by Technology Services and business process owners for

\begin{flushleft}
\footnotesize

\textsuperscript{3} Nick Harley, “10 of the most costly software errors in history,” Raygun (blog), May 10, 2014, https://raygun.io/blog/2014/05/10-costly-software-errors-history/.

\end{flushleft}
new, recurring, and emergency changes. Audit objectives also included determining whether system changes were approved, initiated, authorized, tested, and implemented in a timely manner to minimize disruption to City business.

METHODOLOGY

We tested the effectiveness of the change management process of seven applications and selected network components based on their level of criticality. To assess risks associated with change management, we used a variety of audit methodologies, including:

- Analyzing the controls in place to ensure that changes to existing systems are authorized, tested, approved, properly implemented, and documented
- Reviewing the City’s 2011 Gartner Report on Information Technology Process Maturity Assessment and evaluating process maturity growth
- Using data analytics to compare the listing of both current and former employees against the listing of users with the ability to perform changes
- Evaluating system configuration settings supporting security of production software
- Capturing and reviewing software version modification dates
- Reviewing system-generated logs for unauthorized changes to systems
- Interviewing agency staff to understand City change management processes
- Researching best practices, frameworks, and standards for change management policies and procedures from sources including:
  - Information Technology Infrastructure Library (ITIL)
  - Federal Information System Controls Audit Manual (FISCAM February 2009)
  - National Institute of Standards and Technology (NIST)
  - Control Objectives for Information and Related Technology (COBIT)
  - Microsoft and Cisco change control white papers
- Reviewing the Chief Information Officer’s progress in developing and implementing the new change management process
- Reviewing existing Technology Services policies and procedures related to change management
- Interviewing the Director of Service Operations to determine future direction for Information Technology Service Management (ITSM)
- Reviewing relevant audits conducted nationwide, such as the Change Management Audit for Fairfax County, Virginia, through which auditors identified that a quality assurance function had not been established, production data and code were not
adequately safeguarded, and documented change management procedures were not followed

- Obtaining access to change management software to analyze change records
- Observing automated program library controls to determine whether changes can be introduced outside of the process
FINDING

Technology Services Has Not Fully Mitigated the Inherent Risks within the Change Management Process and Continued Improvements Are Needed To Fully Mature the Process

In assessing the City’s information technology (IT) change management process that was established in October 2013, we found that Technology Services has defined and documented the process, trained staff on the process, and begun implementing a disciplined control structure around system and application changes. However, we identified process improvement opportunities related to process maturity and information security.

City Change Management Process Maturity

Technology Services management has described the City’s change management practices historically as the “Wild West.” In 2011, a consultant described the way changes were introduced into the City’s production environment as “chaotic,” after which Technology Services began implementing a change management process. Our audit of this new process showed marked improvements since it was implemented late in 2013.

In 2011, Gartner, a leading IT research and advisory company, performed an analysis to assess Technology Services’ change management practices. Gartner compared Technology Services’ change management process maturity to other state and local government peers. Gartner used a proprietary process improvement framework that resembles the Capability Maturity Model to determine process improvement areas. The outcome of the Gartner assessment rated Technology Services’ change management process between one and two which indicated a maturity in the initial stage meaning the process was ad hoc and not repeatable.

The Capability Maturity Model characteristics (see Figure 2) developed by the Carnegie Mellon Institute, reflect a more mature rating due to improvements made since the 2013 change control implementation date.
This audit assessed the current change management process by performing a comparison of the Gartner analysis to other capability maturity models. We analyzed the newly established change management process and determined that the City has put into place controls around how IT changes are introduced into the City’s systems and applications. During the past year, the change management team developed the change control process and managed its implementation within Technology Services. The new process has improved communication and collaboration within the Technology Services organization and has also encouraged a more customer-oriented focus. However, we identified several areas for improvement.

Although Technology Services has made great strides in improving the change management process, total integration and adoption of the change control process still needs time to develop and mature to achieve a disciplined change management culture.

The City’s Change Management Procedures Lack Certain Important Elements of Best Practices and Standards

We found that gaps exist in the current change management process due to Technology Services not performing a critical review of their process for overall effectiveness. In early 2014, Technology Services initiated the creation of what they call “Playbooks,” which document the processes and standards created for each role in the change management process and establish the common tasks performed by a person in a given role. We compared the City’s Change Management Process document to
best practices, including the Federal Information Systems Controls Audit Manual (FISCAM), National Institute for Standards and Technology (NIST) 800-128, the Information Systems Audit and Control Association’s (ISACA) Control Objectives for Information Related Technology (COBIT), and Cisco and Microsoft change management white papers. Based on this review, we identified seven gaps in developer and information security role documentation. We recommend that the documented change management process be reviewed at least annually.

Additionally, we identified improvements that could be made to the process document to address the seven gaps identified:

1. Requiring manager approval of detailed requirements and specifications
2. Holding vendors accountable for adhering to City change management procedures
3. Documenting definitions of testing environments
4. Documenting testing standards
5. Identifying risk levels
6. Documenting a security risk analysis
7. Requiring additional details to justify emergency changes

These improvements will help ensure that Technology Services moves its current change control process to a fully defined change management process. Therefore, the Technology Services Change Management team should address the gaps between best practices and City procedures to strengthen accountability by setting expectations for approval of changes, standards for testing, identification of security risks, and vendor compliance with City change management processes.

**Performance Measures Are Insufficient To Evaluate Efficiency and Effectiveness of the Change Management Process**

While Technology Services has established some key performance measures, such as identifying some Information Technology Infrastructure Library (ITIL) critical success factors, the change management process is lacking a method by which to measure overall process improvements. Without clear and quantifiable performance indicators, Technology Services cannot measure the effectiveness or determine the success of the change management process.

When the change management process was implemented, specific, measurable, attainable, realistic, and timed metrics were not established. Based on principles from the ITIL framework, a method to measure process improvement, such as identifying critical success factors, would assist Technology Services in determining areas that require progress. Further, to ensure that Technology Services has a robust set of performance metrics, they should measure all five types of performance indicators: inputs, outputs, outcomes, efficiency, and effectiveness. The five measures are defined as follows:
• **Input Measures** – Inputs determine the resources needed to provide specific products or services; e.g., number of change requests received by type, system, or application.

• **Output Measures** – Outputs define what a program or process produces; e.g., total number of system or application changes. Output measures do not indicate whether the program or process goals have been accomplished. They also lack a means to measure quality or efficiency of service provided.

• **Outcome Measures** – Outcomes provide management with a means to determine whether services are meeting established goals. Outcome measures will show where production has increased or decreased in a specific area or goal; e.g., emergency changes have increased by 10 percent over the prior quarter.

• **Efficiency Measures** – Efficiency measures show levels of productivity, ratio of outputs per period of time, or cost per item of output. An efficiency measurement can be used to track and determine the length of time a specific change request takes and determine a cost based on type of change request.

• **Effectiveness Measures** – Effectiveness measures provide the level of effectiveness in which the goals are meeting the expectations of the end user; e.g., the number of errors in the change process that did not meet user acceptance.

Currently, the performance metrics for the change management process only include input and outcome measures. Specifically:

• Number of emergency changes per agency (input)
• Number of unauthorized changes per application (outcome)
• Availability of applications and systems (outcome)
• Outages resulting from changes (outcome)
• Number of changes that had to be backed out due to unsuccessful implementation (outcome)

Accordingly, Technology Services management should develop stronger metrics to identify trends in change management efficiency and effectiveness. Additionally, Technology Services should begin to capture and track incident and problem management data that can be used to produce the results of the efficiency and effectiveness performance measures. Output measures would indicate to management that change goals have been accomplished and would provide assurance of quality and efficiency.

**Emergency Changes Used as a Work around for Poor Project Management**
Our audit identified that Technology Services is making emergency changes through the change management process when a change does not necessarily qualify as an emergency change. We found that this was due to scheduling inefficiencies, inadequate planning, and short notice from stakeholders.

One example of this was activating the online real estate payments in one application through an emergency change. The change was justified as an emergency because it is a revenue-generating system. However, we found that the activation is a recurring annual event, and the change should have been planned in advance to allow time for review by the Change Advisory Board. Technology Services has historically allowed short notice for implementing changes, and has not consistently enforced the bi-weekly Change Advisory Board schedule when customers present change requests at the last minute. Additionally, we found that some emergency changes were reported to the Help Desk and were described as having dire consequences. However, when the record was entered into the change management software, the description of the emergency change had no mention of time criticality or immediate security concern because it was inaccurately transcribed from the initial request to the change record.

Emergency changes bypass the normal change management process and pose a greater risk of disruption to information processing services. Figure 3 shows that more than 20 percent of all changes made to City applications and environments are made as emergency changes. In a 2008 study of General Motors’ ITIL-based change management program, General Motors’ emergency change rate was 10.08 percent while top performers’ average emergency change rate was 7.10 percent and low performers’ average emergency change rate was 22.90 percent.5

The ITIL framework adopted by Technology Services states that emergency changes should be of a time-critical nature or of an immediate security concern. Accordingly, the Technology Services Information Technology Service Management (ITSM) team should ensure that emergency changes are true emergencies, and better educate agency personnel by providing emergency change statistics and trends. Additionally,  

descriptions of emergency changes in the change management software should include a business justification for the emergency classification.

The Configuration Management Database Lacks Important System-Related Information

Change management software product documentation discusses the importance of maintaining a robust configuration management database (CMDB). It provides the user with basic information about the dependencies between and relationships among systems. A CMDB provides information about the functional and physical attributes of the system that should be taken into consideration when a change to that system takes place. Doing so will help to minimize adverse effects to or impacts on other systems as well as the entire system.

Although Technology Services has implemented change management software, population of the CMDB has not been a priority. Performing data entry for each configuration item is time consuming, and Technology Services has preliminary plans to purchase utility software, which would poll configuration items on the network and populate the CMDB using the polling information.

Without a fully populated CMDB, identification, analysis, and resolution of system problems could be prolonged. Routine system changes could cause performance issues with interfacing environments, and the interfacing system owners cannot be identified in advance if they are not identified in the CMDB. The ITIL best practice framework specifies that CMDBs should be used to track all configurable items and their interrelated dependencies, allowing for activities such as root cause analysis, impact analysis, change management, and current versus future state strategy to occur.

Technology Services should either obtain the utility software needed or perform manual entry to populate the CMDB with all pertinent information about configuration items. A formal process should be established to ensure on-going accuracy and completeness of configuration items and use of the CMDB prior to any change to the system.

Information Security Practices around Change Management Controls Need To Be Strengthened

We found three areas where access controls within the change management structure could be strengthened to improve overall system and application security.

Access Privileges Lack Accountability for Application Changes
Under a mature change management process, in order to make a change to an application, an individual must have special privileges that enable him or her to overwrite the code to modify an application. Log files can be used to trace application changes back to an individual. Should an unauthorized application change occur, administrators of the application could review the log file to determine who made the change.

Several of the applications within the scope of this audit use a shared service account to perform application changes. We found that Technology Services did not establish a method by which to identify the individual who made a change to these production applications. An unauthorized change to the application could result in a disruption in processing, prolonged downtime, and loss of productivity. FISCAM best practice requires that identification and authentication should be unique to each user.

To enforce accountability, Technology Services should establish a process over all shared service accounts. Additionally, an alert should be issued if they are used, since this is a control override and second-level review should occur to ensure that the person performing the task is the person authorized to do so.

There Is No Formal Process for Password Management for Shared Service Accounts

We found that Technology Services has a shared file containing the passwords to some shared service accounts that allow users to make system changes. Some of the individuals who have access to the shared file or have knowledge of the passwords contained in the file have either separated from the City or shifted roles. Therefore, knowledge of these passwords may have been retained by individuals who no longer perform application changes. There is no way to determine all of the individuals who have access to this shared password file. The audit further found that these passwords to shared service accounts are not updated on a regular basis.

This condition occurred because a formal process was never established to control the use and access of this password file. The City’s Acceptable Use Policy states that account use should be restricted to those with a business need. An unauthorized change to an application could result in a disruption in processing, prolonged downtime, and loss of productivity.

Therefore, Technology Services management should establish a process to control who has access to shared service account passwords, and the passwords should be changed periodically. FISCAM requires password changes every thirty to ninety days, depending on the level of sensitivity.

Developers and Former Employees Have Unnecessary Access to the Application Production Environment

Our audit identified ten developers with system access that gave them the ability to move code into the application production environment without review or approval. This direct access was allowed to occur prior to the implementation of the change management process in 2013. We have reasonable assurance to believe that
developers did not take advantage of this unnecessary access. However, unauthorized changes bypass the change management process and could introduce code that could disrupt or harm City data or systems. Best practice suggests that developers should not have access to the production environment.

Additionally, we identified nine former employees who retained access to the application production environment. Additional audit work confirmed that compensating controls exist, which prevented these individuals from making application changes. However, had those compensating controls failed, it is possible that the individuals could have made application changes when they were no longer authorized to do so. This occurred because a formal process was never established to perform periodic access reviews. The City’s Acceptable Use Policy states that account use should be restricted to those with a business need.

Segregation of duties is a security method used by IT organizations to manage potential conflicts of interest. Developers should not have the ability to develop and program an application change while also having the ability to install that change into the application production environment. This could introduce application changes that bypass key change management stages, such as testing, approval, and error correction. Figure 4 shows the analyst and developer roles within the change management process and the importance of segregating these roles.

Figure 4: IT Changes Segregation of Duties

Technology Services management should remove developer access to the application production environment and establish a documented process to perform periodic access reviews, taking into account all steps in the change management life cycle to ensure proper segregation of duties. As part of this periodic access review, Technology Services should ensure that access is removed for former employees.
RECOMMENDATIONS

We offer the following recommendations to improve the City’s change management process in the areas of process maturity and information security.

1.1. **Improve Procedures** – The Technology Services ITSM team should incorporate additional best practices into their change management practices, and should verify that Playbooks contain key responsibility definitions for developer and information security roles.

1.2. **Improve Metrics** – Technology Services management should develop stronger metrics to identify trends in change management effectiveness.

1.3. **Emergency Changes** – The Technology Services ITSM team should limit agencies' implementation of changes on an emergency basis to changes that are true emergencies. The ITSM team should provide emergency change statistics and trends to agency management to discourage classifying comprehensive changes as emergencies.

1.4. **Improve Emergency Change Record Documentation** – Technology Services management should ensure that descriptions of emergency changes in the change management software include a business justification for the emergency classification.

1.5. **Baseline Configuration Items** – The Technology Services ITSM team should populate the configuration management database with all pertinent information about configuration items. A procedure should be developed to ensure that all configuration item information is complete, accurate, and updated.

1.6. **Establish User Accountability** – Technology Services management should ensure that application changes performed by system administrators are monitored by someone independent of the system administrator function or the person who implemented the change, and should be performed on a periodic basis. Additionally, individuals should use their own accounts to perform changes to the application to establish user accountability.

1.7. **Password Controls** – Technology Services management should ensure that passwords used to control shared service accounts are periodically changed.

1.8. **Remove Developer Access** – Technology Services management should ensure that developer access is removed from the production application servers.

1.9. **Remove Former Employee Access** – Technology Services management should ensure that former employee accounts are removed from the production application servers.
1.10. **Periodic Reviews** – Technology Services management should establish a process to perform periodic reviews of access to production to ensure that the appropriate users are authorized to have access to perform application changes. Reviews should take into account former employee access, developer access, and users without a business purpose.
November 7, 2014

Mr. Kip R. Memmott, MA, CGAP, CRMA
Director of Audit Services
Office of the Auditor
City and County of Denver
201 West Colfax Avenue, Dept. 705
Denver, Colorado 80202

Dear Mr. Memmott:

The Office of the Auditor has conducted a performance audit of Change Management Practices.

This memorandum provides a written response for each reportable condition noted in the Auditor’s Report final draft that was sent to us on October 21, 2014. This response complies with Section 20-276 (c) of the Denver Revised Municipal Code (D.R.M.C.).

AUDIT FINDING 1

Technology Services Has Not Fully Mitigated the Inherent Risks within the Change Management Process and Continued Improvements Are Needed To Fully Mature the Process

RECOMMENDATION 1.1

Improve Procedures – The Technology Services ITSM team should incorporate additional best practices into their change management practices, and should verify that Playbooks contain key responsibility definitions for developer and information security roles.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.1

Technology Services will include applicable best practices into our change management processes and verify that documentation including Playbooks contain key responsibility definitions for developer and information security roles.
RECOMMENDATION 1.2
Improve Metrics – Technology Services management should develop stronger metrics to identify trends in change management effectiveness.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>May 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.2
Technology Services will develop stronger metrics, including additional critical success factors and key performance indicators, to measure the effectiveness of the change management process.

RECOMMENDATION 1.3
Emergency Changes – The Technology Services ITSM team should limit agencies’ implementation of changes on an emergency basis to changes that are true emergencies. The ITSM team should provide emergency change statistics and trends to agency management to discourage classifying comprehensive changes as emergencies.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>March 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.3
Technology Services will encourage more lead time on planning for changes with the agencies and educate the agency liaisons on the importance of proper classification of changes.

RECOMMENDATION 1.4
Improve Emergency Change Record Documentation – Technology Services management should ensure that descriptions of emergency changes in the change management software include a business justification for the emergency classification.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>February 28, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.4
Technology Services will ensure that descriptions of emergency changes in the change management software include a business justification for the emergency classification.
**RECOMMENDATION 1.5**

Baseline Configuration Items – The Technology Services ITSM team should populate the configuration management database with all pertinent information about configuration items. A procedure should be developed to ensure that all configuration item information is complete, accurate, and updated.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>June 30, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.5

Technology Services will develop a procedure to ensure that all configuration item information in the configuration management database is complete, accurate, and updated. This procedure will be used to populate the configuration management database.

**RECOMMENDATION 1.6**

Establish User Accountability – Technology Services management should ensure that application changes performed by system administrators are monitored by someone independent of the system administrator function or the person who implemented the change, and should be performed on a periodic basis. Additionally, individuals should use their own accounts to perform changes to the application to establish user accountability.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>July 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.6

Technology Services will begin reviewing application change logs on a periodic basis for changes performed by system administrators. Where technically feasible, Technology Services will use individual accounts to perform application changes in order to establish user accountability.
**RECOMMENDATION 1.7**  
**Password Controls** – Technology Services management should ensure that passwords used to control shared service accounts are periodically changed.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>April 30, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.7**  
Technology Services management will develop a process based on best practices to ensure that passwords used to control shared services accounts are periodically changed.

**RECOMMENDATION 1.8**  
**Remove Developer Access** – Technology Services management should ensure that developer access is removed from the production application servers.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>October 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

**Narrative for Recommendation 1.8**  
Technology Services will immediately remove developer access from production application servers for those accounts that have been identified as a result of this audit. This access will be removed by December 31, 2014.

For all other existing applications, Technology Services will establish a roadmap and process to transition administrative responsibilities from developers to application administrators by May 31, 2015. The transition of administrative responsibilities will be completed by October 31, 2015.

**RECOMMENDATION 1.9**  
**Remove Former Employee Access** – Technology Services management should ensure that former employee accounts are removed from the production application servers.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>December 31, 2014</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>
Narrative for Recommendation 1.9
The accounts were disabled upon the employees’ separation. Technology Services will remove these artifacts from the production application servers.

RECOMMENDATION 1.10
Periodic Reviews – Technology Services management should establish a process to perform periodic reviews of access to production to ensure that the appropriate users are authorized to have access to perform application changes. Reviews should take into account former employee access, developer access, and users without a business purpose.

<table>
<thead>
<tr>
<th>Agree or Disagree with Recommendation</th>
<th>Target date to complete implementation activities (Generally expected within 60 to 90 days)</th>
<th>Name and phone number of specific point of contact for implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agree</td>
<td>May 31, 2015</td>
<td>Alena Gouveia 720-913-4964</td>
</tr>
</tbody>
</table>

Narrative for Recommendation 1.10
Technology Services will establish a process to perform periodic reviews of access to production. These reviews will include consideration of appropriateness based on job responsibilities, developer access, and former employee access.

Please contact Alena Gouveia at 720-913-4967 with any questions.

Sincerely,

Frank Daidone
Chief Information Officer

CC:
Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer
Ms. Janice Sinden, Chief of Staff
Ms. Beth Machann, Controller
Ms. Audrey Donovan, City Auditor’s Office
Ms. Shannon Kuhn, City Auditor’s Office
Ms. Jacqueline Boline, City Auditor’s Office
Mr. Nicholas Jimroglou, City Auditor’s Office
Mr. Stephen E. Coury, Chief Information Security Officer
Mr. Alena Gouveia, Manager of IT Governance