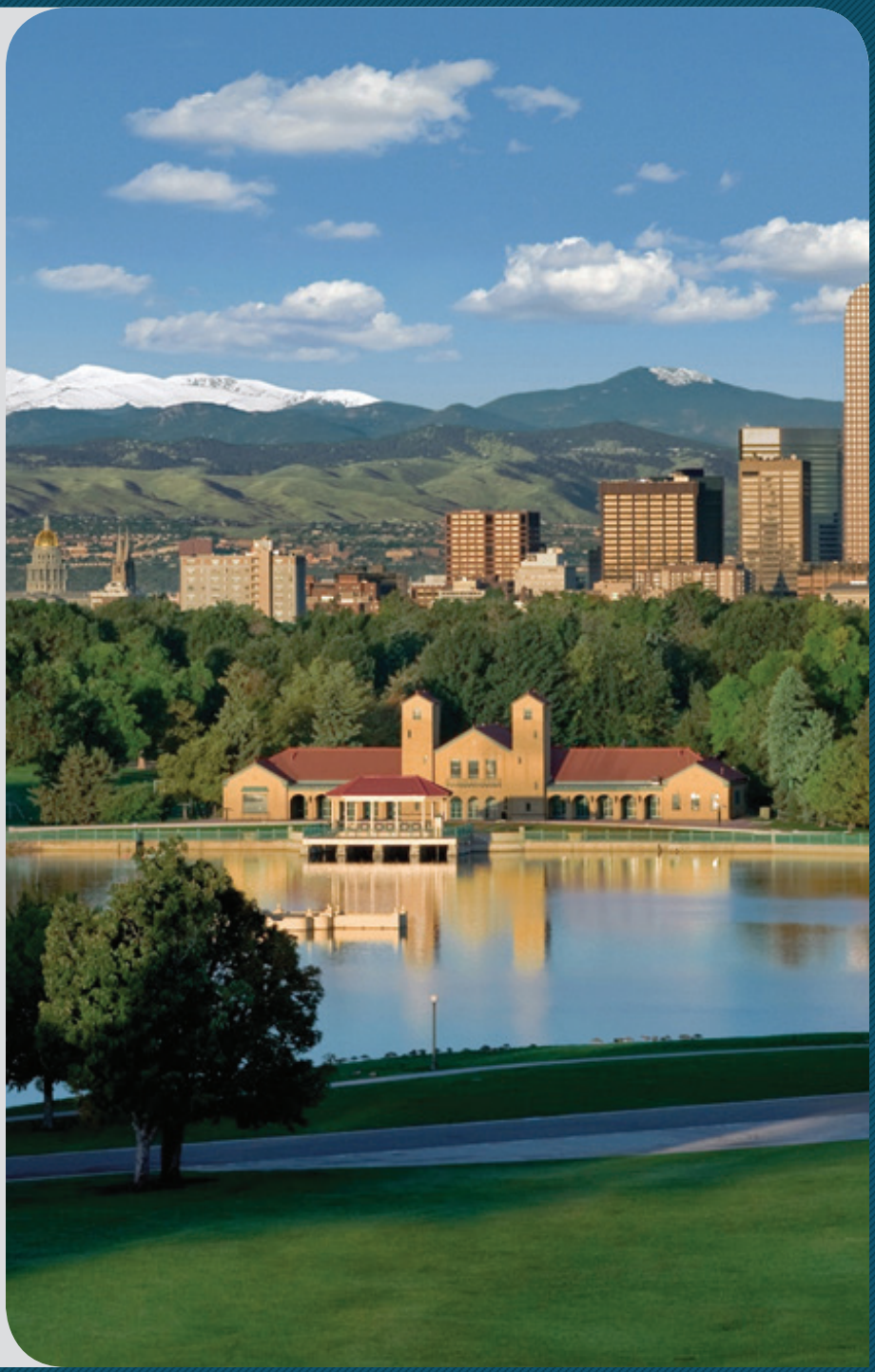
FOLLOW-UP REPORT
Change Management Practices

May 2016



Office of the Auditor
Audit Services Division
City and County of Denver

Timothy M. O'Brien, CPA
Denver Auditor

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 currently consists of six 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

Timothy M. O'Brien, CPA, Chairman
Rudolfo Payan, Vice Chairman
Jack Blumenthal
Leslie Mitchell
Florine Nath
Charles Scheibe
Ed Scholz

Audit Management

Valerie Walling, CPA, CMC®, Deputy Auditor
Kip Memmott, MA, CGAP, CRMA, Director of Audit Services

Audit Staff

Shannon Kuhn, CISA, IT Audit Supervisor,
Nick Jimrolgou, CISA, IT Lead Auditor,
Karin Doughty, CISA, IT Senior Auditor,
Tyler Kahn, IT Senior Auditor

You can obtain copies of this report by contacting us:

Office of the Auditor
201 West Colfax Avenue, #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
Report number: **A2014-12**

City and County of Denver

201 West Colfax Avenue, #705 • Denver, Colorado 80202

720-913-5000 • Fax 720-913-5253 • www.denvergov.org/auditor

Timothy M. O'Brien, CPA
Auditor

May 5, 2016

Scott Cardenas, Chief Information Officer
Technology Services
City and County of Denver

Re: Audit Follow-Up Report

Dear Mr. Cardenas:

In keeping with professional auditing standards and the Audit Services Division's policy, as authorized by D.R.M.C. § 20-276, our Division has a responsibility to monitor and follow-up on audit recommendations to ensure audit findings are being addressed and to aid us in planning future audits.

This report is to inform you that we have completed our follow-up effort for the Change Management Practices audit issued November 20, 2014. Our review determined that Technology Services has adequately implemented nine of the ten recommendations made in the audit report. Despite Technology Services' efforts, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. As a result, the Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

For your reference, this report includes a Highlights page that provides background and summary information on the original audit and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation.

This concludes audit follow-up work related to this audit. I would like to express our sincere appreciation to you and to Technology Services personnel who assisted us throughout the audit and follow-up process. If you have any questions, please feel free to contact me at 720-913-5000 or Shannon Kuhn, Internal Audit Supervisor, at 720-913-5159.

Denver Auditor's Office

Timothy M. O'Brien, CPA
Auditor

Change Management Practices
May 2016

Status

The Technology Services Department (Technology Services) has implemented nine out of the ten recommendations made in the November 2014 audit report.

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.

REPORT HIGHLIGHTS

Highlights from Original Audit

Our audit showed marked improvements to the change management process since it was implemented in 2013. Technology Services had purchased change management software, established an Information Technology Service Management (ITSM) Team, and 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 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 needed to be updated to include suggested items contained in best practice frameworks.
- Performance metrics and third-party service level agreements had not been fully developed.
- Existing controls and processes for emergency changes needed to be enforced to prevent inappropriately prioritizing emergency change requests and approvals.
- The Configuration Management Database needed to 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 needed to be strengthened.
- Procedures needed to be established for reviewing and monitoring privileged accounts.

Findings at Follow-up

Technology Services has developed policies and procedures for the change management process that include best practices, information technology security elements, and roles and responsibilities for key staff. Metrics were developed to determine the success of the Change process. Agency personnel have been educated on providing business justifications and planning for emergency changes. However, five out of seven developers still inappropriately retain access to production application servers. They are still working on a project with an unspecified end date.

For a complete copy of this report, visit www.denvergov.org/auditor
Audit Contact Person: Shannon Kuhn |720.913.5159| ShannonKuhn@denvergov.org

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
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			
1.1	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.	Technology Services has incorporated best practices, such as the Information Technology Infrastructure Library (ITIL), into its change management processes. Playbooks, or process guides, were created to document key responsibilities for developer and information security roles.	**Implemented**
1.2	Technology Services management should develop stronger metrics to identify trends in change management effectiveness.	Technology Services developed stronger metrics that measure the effectiveness of the change management process. Metrics that were developed include critical success factors and key performance indicators. Management regularly reviews these performance metrics to monitor the success of the change management process.	**Implemented**
1.3	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.	Technology Services has educated agencies about the importance of allowing sufficient lead time when requesting changes to discourage the use of using emergency changes and educated agency liaisons on the importance of proper classification of changes. The number of emergency changes has decreased to 12 percent as a result of Technology Services efforts.	**Implemented**
1.4	Technology Services management should ensure that descriptions of emergency changes in the change management software include a business justification for the emergency classification.	Technology Services educated agency liaisons on adding descriptions of emergency changes in the change management software, including a business justification for any change that is classified as an emergency.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.5	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.	Technology Services established a process specific to populating the change management database. It covers the roles and responsibilities for the parties involved in maintaining and updating the database. All items within the database are identified and controlled. Additionally, each item lists the version in use, attributes, and relationships to other configuration items. When a new item needs to be added to the database, a form must be filled out and reviewed by the team that manages the Change Management Database. This process adds to the accuracy of the data and has reporting capabilities.	**Implemented**
1.6	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.	Technology Services has developed a policy for reviewing application change logs on a periodic basis. This helps to provide guidance for the Application Service Owner to perform a periodic review when changes to applications are required. Additionally, a process has been developed to ensure that program changes are reviewed prior to being implemented and the review is conducted by is someone independent of the system administrator function.	**Implemented**
1.7	Technology Services management should ensure that passwords used to control shared service accounts are periodically changed.	Technology Services has developed a process to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of changing the passwords for administrator access.	**Implemented**

Recommendations: Status of Implementation

	Recommendation	Auditee Action	Status
1.8	Technology Services management should ensure that developer access is removed from the production application servers.	Technology Services has established a process to transition administrative responsibilities from developers to application administrators. Two out of seven developers identified in the original audit were remediated, however the remaining five developers still retain access to production systems. The five developers who have production access are currently working on a project with an unspecified timeframe.	**Agreed, Not Implemented**
1.9	Technology Services management should ensure that former employee accounts are removed from the production application servers.	Technology Services removed former employee accounts with access to the production servers as identified in the original audit.	**Implemented**
1.10	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.	Technology Services established a process to perform periodic reviews of access to production. The initial review encompassed privileged accounts for systems identified in the original audit. Technology Services plans to expand the reviews to include additional systems.	**Implemented**

Conclusion

For our follow-up work, we performed the following procedures to validate the auditee's response:

- Interviewed key personnel to gain an understanding of the revisions to the change management policy and procedures
- Reviewed change management policy and process documents for adherence to best practice standards, roles and responsibilities for key personnel, and security incident procedures
- Analyzed a sample of ServiceNow change tickets and emergency change tickets from March 31, 2015, to February 9, 2016, to determine whether more planning had occurred in an effort to decrease the number of emergency changes
- Inspected the ServiceNow change management database for entries that pertained to applications, hardware, operating systems, hardware platforms, and relationships to other applications
- Performed a review of developers with access to selected application production environments
- Reviewed the process for changing the shared service account password ensuring that the password was protected from unauthorized use and changed on a frequent basis.
- Inspected the password application to determine whether the password was last changed in the first quarter of 2016
- Obtained privileged access review and confirmed user access was removed as indicated by review

While Technology Services has implemented the majority of recommendations made in the Change Management Practices audit report, one has yet to be fully implemented. Despite Technology Services' efforts to implement Recommendation 1.8, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. Five out of seven developers retain access to the production environment, which allows them to make changes without adhering to the change management process. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

On behalf of the citizens of the City and County of Denver, we thank staff and leadership from Technology Services for their cooperation during our follow-up effort and their dedicated public service.