OFFICE OF THE CITY AUDITOR

COLORADO SPRINGS, COLORADO

13-18
City of Colorado Springs
Database Security Audit Report

October 2013

Office Of The City Auditor
Colorado Springs, Colorado

13-18
City of Colorado Springs
Database Security Audit

October 2013

Purpose

The purpose of this audit was to provide management with an independent assessment relating to the effectiveness of the configuration and security of the Relational Database Management System (RDBMS) environments used by departments within the City's computing environment.

Highlights

Our audit indicated that most of the configuration and security controls over the RDBMS environments were effective. However, we concluded that some of the controls needed to be improved.

To accomplish our audit objectives, we interviewed management and staff. We reviewed policies and procedures to obtain an understanding of the internal control structure. We also tested settings within the RDBMS environments.

This audit focused on the configuration of the RDBMS environments supporting critical application systems that were identified in the Information Technology (IT) Inventory project conducted in 2011. The audit did not include the application systems that utilized the RDBMS. The audit also did not include the operating systems of the servers that hosted functionality used to access the information in the databases. This audit did not include the physical security of the servers that hosted functionality used to access the information in the databases.

At the time of our audit, the City's Department of IT supported two different RDBMS technologies. Both were tier 1 database software products. The application system used by one of the databases was developed by a

(Continued on page 2)

Management Response

The Colorado Springs Department of Information Technology generally agrees with the observations and recommendations in this report. Please see the report body for their detailed responses.

Recommendations

1. The City develop a written data classification standard that can be applied by City IT in the development and implementation of a data security policy and procedures.
2. Require users to periodically change their passwords if a legacy application system will support such.
3. City IT develop an appropriately documented plan that addresses the recovery of the databases.
4. Rotate copies of backup data created from the databases to an offsite location in a more appropriate timeframe.
5. City IT develop and implement a policy and procedures that adequately control the request and approval of changes to the database environments and data in the databases.
6. The new model for handling database links be documented and implemented to convert all

(Continued on page 2)

(Highlights continued from page 1)

department within the City a number of years ago. Support of this legacy application, the data and the database was transferred to City IT during the City-wide consolidation of the IT function in 2008.

City IT had standardized on a single RDBMS technology as the primary product of choice for use within the City's departments. There was a project underway to replace the legacy department developed application with commercial off the shelf (COTS) software. This project required the COTS software to use the RDBMS technology chosen as the primary product of choice by City IT.

Because this project was underway, we noted City IT preferred to utilize resources to replace the legacy application, instead of continuing to enhance and maintain the application. Minimal effort was also being expended on support of the database. The RDBMS technology was supported by a vendor during our audit. However, that support was scheduled to expire within 18 months. We were mindful of this change as we reviewed the database environment used by the department developed application.

(Recommendations continued from page 1)

existing links to the new model.

7. City IT research and disable as many generic userids defined to the database as possible.

Office of the City Auditor
Public Report

Date: October 9, 2013

To: President King, President Pro-Tem Bennett, and Members of City Council

Re: 13-18 City Database Security Audit

We conducted an audit of the two primary Relational Database Management System (RDBMS) environments utilized by the City of Colorado Springs.

The objective of this audit was to provide management with an independent assessment related to the effectiveness of the configuration and security of the RDBMS technology. This technology was used by departments within the City's computing environment and supported by the City's Department of Information Technology. This audit focused on the configuration of the RDBMS environments supporting critical application systems that were identified in the Information Technology (IT) Inventory project conducted in 2011. The audit did not include the application systems that utilized the RDBMS. The audit also did not include the operating systems of the servers that hosted functionality used to access the information in the databases. This audit did not include the physical security of the servers that hosted functionality used to access the information in the databases.

Our audit indicated that most of the configuration and security controls over the RDBMS environments were effective. However, we concluded that some of the controls needed to be improved. We identified seven main observations and have detailed our recommendations for each. They are listed in the attached report.

As always, feel free to contact me if you have any questions.

Sincerely,

Denny L. Nester, MBA CPA CIA CGFM CFE CGAP

City Auditor

Cc: Mayor Steve Bach
Laura Neumann, Chief of Staff
Joe Palmer, Chief Information Officer
Jesse James, Deputy Chief Information Officer
Mary H. Weeks, IS Application Manager
Scott Campbell, IS Supervisor

REPORT DETAILS

PURPOSE AND SCOPE

We performed an audit of the security and configuration settings of the two primary Relational Database Management Systems (RDBMS) utilized by departments within the City of Colorado Springs and supported by the City's Department of Information Technology (City IT.) The objective of this audit was to provide management with an independent assessment relating to the effectiveness of the configuration and security of the RDBMS technology used within the City's computing environment. This audit focused on the configuration of the RDBMS technology supporting critical application systems that were identified in the Information Technology Inventory project conducted in 2011.

This audit did not include the application systems that utilized the RDBMS. The audit also did not include the operating systems of the servers that hosted functionality used to access the information in the databases. This audit did not include the physical security of the servers that hosted functionality used to access the information in the databases.

BACKGROUND

Definitions:

Database: an integrated collection of data records, files and other objects.

Data Base Administrator (DBA): an individual or group of individuals responsible for the installation, configuration, administration, monitoring and maintenance of databases.

Database Management System (DBMS): a software package that controls the creation, maintenance and use of a database.

Relational Database Management System: a database management system that utilizes relationships within the data to maintain the information across multiple tables of information.

The audit of database configurations ensures management that the RDBMS portion of the application platform that supports the various applications is secure.

In the enterprise, there can be multiple computing platforms for the servers that execute essential business applications. This situation is also true for the database servers that manage the massive databases used to store business data. This also applies to the web servers that provide the public face of the business for transaction processing, both internally to employees and externally to citizens. Generally accepted standards of control recognize that the source of the RDBMS database distribution be known and that controls provide reasonable assurance that only authorized and tested functions, processes, and configuration changes enter the production environment. The failure to properly configure the RDBMS technology could result in the inability of the City to execute its critical business processes and /or the inability to adequately protect the City's information from improper disclosure.

At the time of our audit, City IT supported two different RDBMS technologies. Both were tier 1 database software products. The application system used by one of the databases was developed by a department within the City a number of years ago. Support of this legacy application, the data and the database was transferred to City IT during the City-wide consolidation of the IT function in 2008.

City IT had standardized on a single RDBMS technology as the primary product of choice for use within the City's departments. There was a project underway to replace the legacy department developed application with commercial off the shelf (COTS) software. This project required the COTS software to use the RDBMS technology chosen as the primary product of choice by City IT.

Because this project was underway, we noted City IT preferred to utilize resources on replacing the legacy application instead of continued enhancement and maintenance of that application. Minimal effort was also being expended on support of the database. The RDBMS technology was supported by a vendor during our audit. However, that support was scheduled to expire within 18 months. We were mindful of this as we reviewed the database environment used by the legacy department developed application.

CONCLUSION

Our audit indicated that most of the configuration and security controls over the RDBMS environments were effective. However, we concluded that some of the controls needed to be improved. We identified seven main observations and have detailed our recommendations for each on the pages that follow.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

OBSERVATION 1 –CITY-WIDE DATA CLASSIFICATION STANDARD, DATA SECURITY POLICY AND PROCEDURES WERE INADEQUATE

City IT had not documented a City-wide data classification standard. This type of standard should apply throughout the enterprise and define the criticality and sensitivity of enterprise information. It should also address the details about data ownership, the definition of appropriate security levels and protection controls as well as briefly address data retention and destruction requirements.

Because a City-wide data classification standard did not exist, a written data security policy and appropriate procedures also did not exist to aid City IT staff in the determination of how to properly secure information within the databases. This type of policy and procedures should ensure the integrity and consistency of all data stored in electronic form. We did note that City IT staff were aware of such data security regulations as the Health Insurance Portability and Accountability Act of 1996 (HIPPA) and the need to properly secure Personally Identifiable Information (PII).

Processes, administrative policies and procedures should be in place for information security. They should include the definition and assignment of roles for managing information security. The management of information security should be at a high enough level in the City so that management security actions are in line with business requirements. Without appropriate governing policies and procedures, there is risk that information that should be protected could be disclosed or modified.

AUDITOR'S RECOMMENDATION

We recommend that the City develop a written data classification standard. The approved data classification standard should be applied by City IT in the development and implementation of a data security policy and procedures.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We are in the process of creating and implementing an information security program that will include data classification standards as part of a set of data security policy and procedures.

OBSERVATION 2 – A LEGACY DATABASE HAD WEAK PASSWORD CONTROLS ON USERIDS

We noted that userids setup for access within one legacy application and database environment were given a default password that was the same for all userids that had been established. We also noted that the application did not require the owner of the userid to change the password upon initial access of the application. It appeared that processes developed over time had not included the requirement of users to periodically change their passwords. This situation existed even though users were instructed on how to change the userid password at the time they were given their initial password.

Userid passwords should never be known by anyone other than the owner of the userid. This control prevents unauthorized personnel from gaining inappropriate access to information or being able to improperly modify data. It also provides the ability for personnel to be held accountable for their actions.

Users should be required to change the password upon initial use. Users should also be required to periodically change their passwords. Changing passwords will help thwart the possibility of passwords being guessed.

AUDITOR'S RECOMMENDATION

We recommend that an assessment be made to determine if users can be required to change their passwords through the legacy application system. If possible, we recommend users be required to change their passwords the first time they log into the application system. We also recommend that users be required to periodically change their userid passwords.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We will perform an assessment of the one legacy application system using this security model to determine if users can be required to change their passwords by the end of October 2013.

OBSERVATION 3 – WRITTEN RECOVERY PLANS FOR SOME DATABASES WERE INADEQUATE

We observed that a written recovery plan for some of the databases reviewed did not exist.

The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, utilizing offsite backup storage and providing periodic continuity plan training. An effective continuous service process minimizes the probability and impact of a major IT service interruption on key business functions and processes.

The City's Information Technology Security Policies Manual required that enterprise-level IT managers and system administrators have a documented plan or procedure to provide for disaster response for enterprise-level IT assets and systems. The databases reviewed were enterprise-level IT assets. Documentation provided appeared to be sufficient for knowledgeable individuals to create and restore the databases. However, that documentation was not written from a recovery perspective. And the electronic location of this documentation may not be known by IT management and other IT support individuals that may need such documentation for recovery of the databases. This places an increased dependency upon key individuals that may not be available when necessary. It could lead to a failure to recover IT systems and services in a timely manner.

AUDITOR'S RECOMMENDATION

We recommend that an appropriately documented recovery plan be developed for the databases reviewed. Once developed, the plan should be periodically maintained to ensure it can be utilized for the then current databases. The plan should also be periodically tested to ensure that it actually supports the recovery of the databases. The plan should be stored in an appropriate form and location to ensure it can be retrieved when necessary by individuals who may not be aware of its existence.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We will document the database recovery plan and test the plan to ensure that it supports the recovery of databases by the end of October 2013.

OBSERVATION 4 –TIMELINESS OF OFFSITE ROTATION OF DATABASE BACKUPS WAS INADEQUATE

The DBAs had processes in place that created backup data sets for some of the databases on a file server. The file server was located in the City's primary data center along with the database servers. The backup tapes containing the most recent copies of the information stored on the file server and database servers were retained in the data center for up to seven days before the tapes were rotated to an offsite location.

If an event were to occur that rendered the City's primary data center unusable, the current versions of the backup data stored on the file server could be destroyed along with the databases on the database servers. At the same time, the backup tapes containing the most recent full backup tape set and all incremental backup tape sets of the database and the file servers could also be destroyed. The recovery from tapes stored at the offsite location would result in a recovery point in time between one day and seven days prior to the disaster event.

In order to provide an adequate recovery of the IT operations used by City departments, the most recent backup data should be available from an offsite location in the event of the physical destruction of the primary data center.

AUDITOR'S RECOMMENDATION

We recommend copies of all backup information created from the databases be stored at an offsite location as soon as practical after the backup cycle has completed.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We will ensure that tape backups from databases are delivered to an offsite location on a daily basis by the end of September 2013.

OBSERVATION 5 –WRITTEN POLICIES AND PROCEDURES GOVERNING CHANGES TO DATA IN THE DATABASES AND DATABASE ENVIRONMENTS WERE INADEQUATE

There was no formal documented policy or written procedures governing the emergency access of the database environments by the DBAs. The DBAs indicated that emergency access was only used when time was of the essence. Normally the DBAs utilized the Request for Change process. There also was no formal documented policy or written procedures governing emergency changes to data or the manual backout of data entered by users in the databases. There also was no logging of access made by the DBAs to one of the databases. Additionally, the method for handling and tracking the manual rollback of data entered by users in a database was an informal process.

Formal change management procedures should be established to handle all requests for changes (including data changes, maintenance and patches.) Processes should be established for defining, testing, documenting, assessing and authorizing emergency changes to data and the database environments. Logging access of the DBAs adds a level of control that would help in monitoring their access and what changes had occurred.

City IT had not formally documented these procedures or overarching policy. The number of rollback changes to the data appeared to be rare. It also appeared that the data owners were asked to approve the rollback changes, when appropriate.

Without a documented policy and procedures routine changes to database environments and data in the databases may be occurring under the pretense that the change is an emergency. And the change request to rollback data may not always be recorded and approved by the data owners.

AUDITOR'S RECOMMENDATION

We recommend

- Policy be developed and implemented that directs how changes to the database environments and data in the databases be requested, documented and approved.
- Once the policy has been developed and approved, we recommend appropriate procedures be developed and implemented to aid in the control of the requests to manually rollback data within the database. These procedures should also govern the emergency access to the database environments and any changes made during an emergency situation.
- Access to the databases by the DBAs be logged.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We will develop and implement a policy governing database changes. We then will create and implement a procedure to control changes to the database, including logging, by the end of December 2013.

OBSERVATION 6 – AN OUTMODED METHOD WAS USED TO LINK DATABASES

We noted a database link between two separate databases utilized an outmoded method for the link. We also noted that the DBAs had developed a new model for creating database links; however, it had not been documented.

A link between two databases allows the ‘calling’ database to have access to the data in the ‘called’ database. The reviewed database link provided read-only access to all information within the ‘called’ database. Depending on how the application issuing the call to the ‘called’ database was setup, this database link could be exploited. This exploit could make information in the ‘called’ database available to an unauthorized user.

AUDITOR’S RECOMMENDATION

We recommend that the new model for handling database links be documented. We also recommend the new model be implemented for all existing database links.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We will document the updated model for creating database links, analyze the impact of changing all existing database links, and create a strategy for changing existing database links by the end of December 2013.

OBSERVATION 7 – GENERIC USERIDS EXISTED WITH ACCESS TO A DATABASE

We noted there were 15 generic userids, i.e. userids not readily attributed to a specific user were defined in the legacy database environment. These userids needed to be disabled if possible.

Upon an initial review, City IT staff had indicated that a few of these userids would be disabled. The remainder required further evaluation to ensure no impact to the application system.

If possible, all users and their activity on IT systems and databases should be uniquely identifiable. All user access rights to systems and data should be granted based on business needs and job requirements. Generic userids may be necessary for a variety of reasons. The reason for the existence of generic userids should be documented.

AUDITOR'S RECOMMENDATION

We recommend that generic userids be disabled where possible. The generic userids that cannot be disabled should have documentation indicating why they must exist. We also recommend that written procedures for the periodic review of all userids with access to the database be developed and implemented.

CITY OF COLORADO SPRINGS RESPONSE

We agree with the recommendation. We have already disabled generic userids where possible. We will document why remaining generic userids exist, and prepare and implement written procedures for periodic review of all userids with database access by the end of October 2013.

City Council's Office Of The City Auditor
Colorado Springs, Colorado

About our Office
The mission of the Office of the City Auditor is to provide City Council with an independent, objective and comprehensive auditing program for operations of the City. Our auditing program includes:

- Evaluating the adequacy of financial controls, records and operations
- Evaluating the effectiveness and efficiency of organizational operations
- Providing Council, management and employees objective analysis, appraisals, and recommendations for improving systems and activities

The Office of the City Auditor is responsible for auditing the systems used by the City of Colorado Springs and its enterprises, including Colorado Springs Utilities. We perform a variety of audits for these entities, including financial audits, performance audits, contract audits, construction audits, and information system audits. We also perform follow-up on a periodic basis to monitor and ensure management actions have been effectively implemented.

Authorization and Organizational Placement
Our audits are conducted under the authority of Chapter 1, Article 2, Part 7 of the Colorado Springs City Code, and more specifically parts 703, 705 and 706 of the Code. The Office of the City Auditor is structured in a manner to provide organizational independence from the entities it audits. This independence is accomplished by the City Auditor being appointed by and reporting directly to the City Council.

Audit Standards
The audit was conducted in a manner that meets or exceeds the International Standards for the Professional Practice of Internal Auditing, a part of the Professional Practices Framework promulgated by the Institute of Internal Auditors, with the exception of the requirements under standards 1312 and 1321 to obtain an external quality assurance review once every five years. We do not believe this non-compliance impacted the quality of our audit.

The audit included interviews with appropriate personnel and such tests of records and other supporting documentation as deemed necessary in the circumstances. We reviewed the internal control structure and compliance tests . Sufficient competent evidential matter was gathered to support our conclusions.

City Hall ◆ 107 North Nevada Avenue ◆ Suite 200 ◆ Mail Code 1542
Colorado Springs CO 80901-1575
Tel 719-385-5991 ◆ Fax 719-385-5699 ◆ Reporting Hotline ◆ 719-385-2387
www.SpringsGov.com/OCA