



OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

13-25
Colorado Springs
Utilities Maximo
Application Audit

December 2013



OFFICE OF THE CITY AUDITOR

COLORADO SPRINGS, COLORADO

13-25

Colorado Springs Utilities Maximo Application Audit

December 2013

Purpose

The purpose of this audit was to evaluate the effectiveness of controls related to the Maximo system used by Colorado Springs Utilities. Our audit was focused on controls over source code, database and server security, application recovery, and business continuity.

Highlights

We concluded that overall the controls governing the Maximo application at Colorado Springs Utilities were effective. We have identified three areas where processes and controls could be strengthened. These areas are detailed in the attached report.

The Maximo system was used by Colorado Springs Utilities as a work and resource management system, which includes asset management, time-keeping for employees, accounts payable, work order tracking, and other functions.

The scope of the audit included the Maximo Information Technology (IT) application controls and Colorado Springs Utilities IT general controls. IT general controls are controls that apply to all systems components, processes, and data for a given IT environment. IT application controls are controls over the input, processing, and output functions of an application. During the audit, Colorado Springs Utilities was planning to re-implement a more recent version of the Maximo system. This re-implementation was planned to begin at the end of 2013. This initiative was most likely going to require the redesign of many of the business processes within Colorado Springs Utilities. Therefore, our review was focused on controls and information that was not likely to be modified by the upgrade.

Management Response

Colorado Springs Utilities management was generally in agreement with our recommendations. See the attached report for detailed responses.

Recommendations

1. Prepare a Business Impact Analysis for the Maximo application. Create and maintain business continuity plans which address performing functions without the Maximo application.
2. Expand the Information Protection Program to include sensitive information related to third parties. Ensure that sensitive information is adequately secured in Maximo.
3. Retest the application failover process as scheduled. Develop and follow a procedure to routinely test the failover process of the Maximo application system.

**City Council's
Office of the City Auditor
City Hall
107 North Nevada Ave. 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**



Office of the City Auditor

Colorado Springs Utilities Maximo Application Audit

Date: December 27, 2013

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

Re: 13-25 Colorado Springs Utilities Maximo Application Audit

We conducted an audit of the Maximo application, which was used by Colorado Springs Utilities for asset tracking, resource management, and time entry.

The purpose of this audit was to evaluate the effectiveness of internal controls governing the application. The audit included the Maximo application, as well as Information Technology general and application controls. Colorado Springs Utilities was planning to re-implement the Maximo application beginning the end of 2013. Therefore, the audit was more focused on general controls dealing with the support and maintenance of the application rather than the application controls within the application itself.

We concluded that in general the controls governing the Maximo application were effective. We identified three main observations and have listed our recommendations for each. They are listed in the attached report.

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

Sincerely,

A handwritten signature in black ink, appearing to read "Denny L. Nester".

Denny L. Nester, MBA CPA CIA CGFM CFE CGAP

Cc: Jerry Forte, Chief Executive Officer
Carl Cruz, Chief Customer and Corporate Services Officer
Bill Lopez, Interim General Manager, Information Technology Services Department
Charise Swanson, Manager, Compliance and Risk Mitigation Services
Bruce McCormick, Chief Energy Services Officer
Mason Parsaye, General Manager, Energy Construction, Operations and Maintenance
George Luke, General Manager, Energy Supply Department
John Romero, General Manager, Energy Acquisition, Engineering and Planning
Gary Bostrom, Chief Water Services Officer
Leah Ash, General Manager, Distribution, Collection and Treatment Department
Wayne Vanderschuere, General Manager, Planning, Engineering and Resource Management
Tyler Allison, General Manager, Water System Operations
Steve Kuhr, Manager, Business Continuity Management



Office of the City Auditor
Colorado Springs Utilities Maximo Application Audit

David Padgett, Chief Environment, Health and Safety Officer

Bill Cherrier, Chief Planning and Financial Officer

Dede Jones, General Manager, Financial Services

David Maier, Manager, Enterprise Risk Management Services

Patricia Van Meter, Lead Analyst, Enterprise Risk Management Services



Office of the City Auditor

Colorado Springs Utilities Maximo Application Audit

Report Details	1
Purpose and Scope	1
Background	1
Commendable Practices	1
Conclusion	2
Observations, Recommendations and Responses	3
Observation 1 – A Business Impact Analysis had not been prepared and departments did not have business continuity plans	3
Observation 2 – The Maximo application contained sensitive information related to third parties	5
Observation 3 – Failover testing of the Maximo application had not been regularly performed	6



Office of the City Auditor

Colorado Springs Utilities Maximo Application Audit

REPORT DETAILS

PURPOSE AND SCOPE

The purpose of this audit was to evaluate the effectiveness of controls related to the Maximo system used by Colorado Springs Utilities. Our audit was focused on controls over source code, database and server security, application recovery, and business continuity.

The scope of the audit included the Maximo Information Technology (IT) application controls and Colorado Springs Utilities IT general controls. IT general controls are controls that apply to all systems components, processes, and data for a given IT environment. IT application controls are controls over the input, processing, and output functions of an application. IT application controls include such items as user authentication, authorization, and input verifications. IT general controls include such items as disaster recovery and change management. During the audit, Colorado Springs Utilities was in the process of planning to re-implement a more recent version of the Maximo system. This re-implementation was planned to begin at the end of 2013. This project was most likely going to require the redesign of many of the business processes within Colorado Springs Utilities. Therefore, review of the actual application and the data contained in it was generally excluded from the audit and the general controls over the application were examined instead.

BACKGROUND

The Maximo system was used by Colorado Springs Utilities as a work and resource management system, which included asset management, time keeping for employees, accounts payable, work order tracking, and other functions. The Maximo application was produced by IBM, utilized a relational database management system, used a web interface with the general user population, and used application system servers. The application had been modified by Colorado Springs Utilities to customize it for their business. Information from the Maximo application has been used in performing other audits by this office, but the application itself has not previously been audited.

COMMENDABLE PRACTICES

Information Technology Services had configured the Maximo application to failover to the secondary data center in the event of an issue at the primary data center. This failover process was designed to keep the downtime of the Maximo application to a minimum. As the Maximo application was relied on for daily work by numerous departments and teams at Colorado Springs Utilities, we identified implementing the failover process as a commendable practice.



Office of the City Auditor

Colorado Springs Utilities Maximo Application Audit

CONCLUSION

We concluded that overall the controls governing the Maximo application at Colorado Springs Utilities were effective. We have identified three areas where processes and controls could be strengthened. These areas are listed on the pages that follow.



Office of the City Auditor Colorado Springs Utilities Maximo Application Audit

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

OBSERVATION 1 – A BUSINESS IMPACT ANALYSIS HAD NOT BEEN PREPARED AND DEPARTMENTS DID NOT HAVE BUSINESS CONTINUITY PLANS

We noted that a Business Impact Analysis (BIA) had not been prepared for the Maximo application and individual departments did not have business continuity plans.

A BIA measures the dependence on the system or application by the business operations. Business continuity plans provide instructions which detail how to handle business operations and maintain important functions during the time the application is unavailable for use. Without a BIA and business continuity plans, there is a risk that the recovery objectives for the system may not be appropriate. Additionally, there is a risk that departments may not be able to maintain important functions if the Maximo application is not available.

Information Technology Services (ITS) at Colorado Springs Utilities had negotiated with the Maximo Steering Committee in 2012 to set recovery objectives for Maximo. The Recovery Time Objective (RTO) for the Maximo application was set at 72 hours, and an agreement was made on the Recovery Point Objective (RPO). The RTO represents the maximum amount of time which should pass between an application becoming unavailable and the ability to once again use that application. The RPO is the maximum tolerable period in which data might be lost from an IT service due to a major incident.

The Maximo application was overseen by a Steering Committee and Management Review Team (MRT). The Steering Committee was responsible for prioritizing and deciding what changes and enhancements were made to the Maximo application. The MRT consisted of management level members of divisions and departments which used the Maximo application. The MRT was responsible for providing oversight and governance in respect to the use and maintenance of Maximo.

Multiple departments at Colorado Springs Utilities relied heavily on the Maximo application, including Procurement, Accounts Payable, Payroll, and Materials Management. Many of the departments which used this application provided needed services to other internal departments. During the upcoming re-implementation, these departments could go through business process reengineering, which may change the processes that rely on the Maximo application.

Departments which relied on the Maximo application for completing tasks central to the function of the department should have business continuity plans which specifically addressed the possibility of Maximo being unavailable for the duration of the RTO. Departments reviewed during the audit did not have business continuity plans addressing the unavailability of the Maximo application. Most departments indicated that tasks normally performed with Maximo would cease until the application was restored. As a result, if the Maximo application experienced an outage, multiple internal customers could be left without important services for the duration of the outage.



Office of the City Auditor Colorado Springs Utilities Maximo Application Audit

Normally the RTO and RPO for a system are determined after preparing a BIA. We noted during our review that a BIA had not been prepared for the Maximo application. The absence of both a BIA and business continuity plans make it difficult to accurately evaluate the appropriateness of the 72-hour RTO.

AUDITOR'S RECOMMENDATION

We recommend that Colorado Springs Utilities prepare a Business Impact Analysis for the Maximo application promptly following the re-implementation, and evaluate the Recovery Time Objective and Recovery Point Objective.

In addition, we recommend the Colorado Springs Utilities Management Review Team for the Maximo application oversee the creation of business continuity plans following the completion of the Business Impact Analysis. These plans should address the potential unavailability of Maximo for at least the duration of the Recovery Time Objective to ensure that important functions are maintained.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with the recommendation. Colorado Springs Utilities Management Review Team for the Maximo Application will evaluate the Recovery Time Objective and the Recovery Point Objective as part of the business impact analysis during the re-implementation. The Colorado Springs Utilities Management Review Team for the Maximo Application agrees to evaluate the need for Business Continuity Plans for critical business process flows. These flows will be identified as part of the re-implementation. A plan will be developed to create Business Continuity Plans for identified critical business process flows no later than six months after the completion of the project.



OBSERVATION 2 – THE MAXIMO APPLICATION CONTAINED SENSITIVE INFORMATION RELATED TO THIRD PARTIES

We noted the Maximo application contained sensitive information related to third parties which was not identified as protected under Colorado Springs Utilities Information Protection Program.

Inadequately protected sensitive information increases the risk of identity theft and other fraud. Due to this risk, sensitive information should be stored securely with limited access. Colorado Springs Utilities Information Protection Program defined and protected multiple types of sensitive information. However, the program did not adequately address sensitive information related to third parties.

In addition, it was determined during the review that the Maximo database contained sensitive information related to third parties. Colorado Springs Utilities communicated prior to the issuance of this report that they were in the process of securing and limiting the access of this sensitive information to only authorized users.

AUDITOR'S RECOMMENDATION

We recommend Colorado Springs Utilities expand their Information Protection Program to include the protection of all sensitive information related to third parties.

Once the Information Protection Program has been updated to address sensitive information related to third parties, we recommend Colorado Springs Utilities review and ensure the protection of all sensitive information retained in the Maximo application is adequate.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with the recommendation. While the Information Protection Program broadly addressed confidential information, it did not specifically define "sensitive information related to third parties." Colorado Springs Utilities has added specific language to address this type of information. The revised Information Protection Program will be approved and available by the end of December 2013.

The Maximo security groups have been modified to restrict sensitive third party information. Access is limited to employees that require access to perform their job duties, and the system administration support team. A review of the security changes will be performed by the Compliance and Risk Mitigation Services of Colorado Springs Utilities in the first quarter of 2014.



Office of the City Auditor Colorado Springs Utilities Maximo Application Audit

OBSERVATION 3 – FAILOVER TESTING OF THE MAXIMO APPLICATION HAD NOT BEEN REGULARLY PERFORMED

We noted that routine testing of the failover process had not been completed. This lack of testing created a risk of reduced productivity in departments which relied heavily on the Maximo application. There was also the risk of suspension of department based tasks in the event of a service disruption.

The Maximo application and databases were normally stored at and ran through Colorado Springs Utilities primary data center. The application and database were configured to failover to the secondary data center if there was an issue or outage at the primary data center. As long as the failover process worked correctly and both data centers had not experienced a simultaneous outage, this arrangement ensured that the Maximo application was available for use.

Prior to the beginning of audit work, the Maximo failover process had not been completed or tested in over eighteen months. During the audit, a test of the failover process for some of the technical infrastructure was performed by Colorado Springs Utilities and this test was reported to have been unsuccessful. Colorado Springs Utilities had communicated they were correcting the issue and intended to retest this portion of the failover process by the end of the year. Untested failover routines could lead to a failure to recover the application within the Recovery Time Objective. Therefore, routine testing of all components of the failover process should be performed and any issues encountered should be corrected.

AUDITOR'S RECOMMENDATION

We recommend that Colorado Springs Utilities develop and follow a procedure to routinely test all components of the failover process for Maximo.

In addition, we recommend that Colorado Springs Utilities retest the Maximo application failover process as scheduled, and take action to correct any additional issues.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with the recommendation. A successful failover test occurred on November 13, 2013. Colorado Springs Utilities agrees to perform a failover test on an annual basis.

CITY COUNCIL'S OFFICE OF THE CITY AUDITOR

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.