OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

12-24
Colorado Springs Utilities Data Center Audit Report

December 2012

OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

12-24
Colorado Springs Utilities Data Center Audit

December 2012

Purpose

The purpose of this audit was to evaluate the adequacy of the physical, environmental, safety and security controls of the data centers.

Highlights

We conclude that the physical, environmental, safety and security controls were adequate for the data centers that we reviewed. However, during the course of our audit, we identified areas where improvements could be made to further strengthen controls. These areas are detailed on the pages that follow. The audit included a review of the signage, data center locations, and data center construction; a review of access points, power circuits, and general housekeeping; a review of the physical access controls to the data centers; a review of the environmental systems and fire suppression systems; and a review of the continuity of operations of the primary data center.

To accomplish our audit objectives, we reviewed policies and procedures to obtain an understanding of the internal control structure around the data centers. We interviewed management and staff. We observed operations and we reviewed construction drawings and various manuals that governed the procedures for the proper initiation and approval of access to the data centers. We also reviewed procedures and processes around the maintenance of critical environmental systems. And we evaluated the procedures and processes used to govern the controls of the data centers in the event of an emergency situation.

Management Response

Management was generally in agreement with our recommendations.

Recommendations

1. Evaluate alternatives and implement a solution to reduce the risk of damage to the primary data center due to the fire and explosion hazards nearby.
2. Identify and evaluate alternatives and implement a solution that will reduce the risks to the failover data center due to issues with the facility's infrastructure.
3. Periodically reconcile the listings of media stored offsite with the lists from the offsite storage vendor.
4. Establish processes for the routine inspection, testing and replacement of the hydrogen sensor in the UPS room.
5. Enhance policy and procedures governing the primary data center in the event of an emergency situation.
6. Resolve issues identified during the inspections of the halon and water based fire suppression systems of the primary data center.

(Continued on page 2)

12-24
Colorado Springs Utilities
Data Center Audit

December 2012

(Recommendations continued from page 1)

7. Develop policy and procedures dealing with activated water alarms in the primary data center.

City Council's Office of the City Auditor
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

Office of the City Auditor
Public Report

Date: December 7, 2012

To: President of Council Hente, President Pro-Tem Martin, and Members of City Council

Re: 12-24 Colorado Springs Utilities Data Center

We conducted an audit of the Colorado Springs Utilities primary and failover data centers. The purpose of this audit was to evaluate whether physical, environmental, safety and security controls were adequate for the data centers. The audit included a review of the signage, data center locations, and data center construction; a review of access points, power circuits, and general housekeeping; a review of the physical access controls to the data centers; a review of the environmental systems and fire suppression systems; and a review of the continuity of operations of the primary data center.

We concluded that the physical, environmental, safety and security controls were adequate for the data centers that we reviewed. However, during the course of our audit, we identified areas where improvements could be made to further strengthen controls. We identified seven observations and have listed our recommendations for each. They are detailed in the attached report.

We would like to thank the Colorado Springs Utilities Information Technology Services, Facilities Management, and Security Operations Departments for their time and assistance in completing this audit.

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: Jerry Forte, Chief Executive Officer
Bill Cherrier, Chief Planning and Financial Officer
Carl Cruz, Chief Customer and Corporate Services Officer
Alan Goins, Manager, Facilities and Security Management
James Budnella, Facilities Building Maintenance Supervisor
Vincent Scarsbrook, Lead Analyst, Facilities Business Support
Valerie Schmidt, Managing Principal, Facilities Architect - Engineering
Gabe Caunt, Sr. Project Manager, Facilities Architect - Engineering
Thane LaBarre, Sr. Project Manager, Facilities Architect - Engineering
Dawn Roth, General Manager, Information Technology Services Department
Brian Bleike, IT Project Manager, IT Service Management
Joe Hickert, Manager, ITS Client Support
Jeff Icke, Manager, ITS Collaboration and Security Management

City Council's Office of the City Auditor
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

Cc: (Continued)

Keith Christensen, Systems and Database Lead, ITS Enterprise Server Administration
Jayant Patil, Systems and Database Lead, ITS Enterprise Server Administration
William Lopez, Jr., Manager, ITS Resource Technology Services
Bonnie Moeder, Manager, ITS Enterprise Business Solutions
Gary Bauer, IT Supervisor, ITS Customer Information Systems
David Reinecke, IT Supervisor, ITS Information Security Management
David Maier, Manager, Enterprise Risk Management Services
Patricia Van Meter, Sr. Analyst, Enterprise Risk Management Services

Office of the City Auditor
Colorado Springs Utilities - Data Centers

REPORT DETAILS

PURPOSE

We performed an audit of the Colorado Springs Utilities primary and failover data centers. The purpose of this audit was to evaluate whether physical, environmental, safety and security controls were adequate for the data centers. The audit included a review of the signage, data center locations, and data center construction; a review of access points, power circuits, and general housekeeping; a review of the physical access controls to the data centers; a review of the environmental systems and fire suppression systems; and a review of the continuity of operations of the primary data center.

SCOPE

The scope of the audit included reviewing controls over 1) the structure of the physical data centers and the contents of rooms immediately adjacent to the data centers, 2) equipment, devices, policies, and procedures used to secure the data centers, 3) environmental, safety, security, power, lighting, and signage used in the buildings housing the data centers and in the immediate vicinity of the doorways entering the data centers, and 4) a review of the continuity of operations used for the primary data center.

BACKGROUND

The Office of the City Auditor has not previously conducted an audit of the data centers used at Colorado Springs Utilities. Multiple data centers are used by Colorado Springs Utilities with some being governed by the North American Electric Reliability Corporation's Critical Infrastructure Protection standards developed to improve physical and cyber security for the bulk power system of North America. Our review did not include data centers governed by these standards because of on-going and routine inspections by independent auditors to verify compliance.

A primary data center is used for much of the daily business information processing of Colorado Springs Utilities. A failover data center exists to be used in the event of a catastrophic failure at the primary data center.

COMMENDABLE PRACTICES

We noted two items that we considered to be commendable practices. First, a hydrogen sensor had been installed in the room housing the uninterruptible power supply for the primary data center. Batteries associated with an uninterruptable power supply of this type often discharge hydrogen gas, which is highly combustible when present in large amounts in a contained environment. This room is housed in the same building as the primary data center. This building also contains a significant number of staff. Thus, the buildup of hydrogen gas in a closed room could pose considerable risk to personnel,

equipment, and the facility. We wish to commend Colorado Springs Utilities on the decision to enhance the protection of life and property by installing this hydrogen sensor.

We also noted that it was possible to visibly determine the difference between the halon abort switch and the emergency power off switch; in the past both switches were the same color. Both switches were co-located near an exit to the primary data center and with both having the same color, confusion could have resulted in the event of an emergency situation. And we observed that both switches had been enclosed with covers that would not significantly impede the use of the switches in the event of an emergency. By covering the switches, both switches were better protected from accidental tripping by personnel or equipment moving near-by these switches.

CONCLUSION

We conclude that the physical, environmental, safety and security controls were adequate for the data centers that we reviewed. However, during the course of our audit, we identified areas where improvements could be made to further strengthen controls. These areas are detailed on the pages that follow.

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

OBSERVATION 1 – LOCATION OF THE PRIMARY DATA CENTER

Our review indicated that there were multiple fire and explosion hazards, e.g. diesel fuel and other substances, located in the vicinity of the building that houses the primary data center. This increases risk to the building housing the data center and the information processing that occurs at the data center.

AUDITOR'S RECOMMENDATION

We recommend that Colorado Springs Utilities evaluate alternatives to reduce the risk of impact to the data center from the fire and explosion hazards. One alternative could be to move the data center to a facility that is not as exposed to such fire and explosion hazards. Once a preferred solution is identified, we recommend that the choice be implemented.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with this recommendation and recognizes that the location of the primary data center is at risk to loss of use as a result of hazards identified. However, a number of fire detection and prevention systems have been installed, and safety practices initiated to mitigate any catastrophic loss of this facility. Colorado Springs Utilities has also included in its capital plan for 2013 to begin relocation and expansion of its secondary data center to allow for enhanced redundancy of its systems should loss of the primary data center occur. Earlier this year, Colorado Springs Utilities contracted with Enabled Energy, Inc., to assist with evaluating "buy vs. build" alternatives to house a new secondary data center. The preferred approach and business case will be finalized in the second quarter of 2013 with implementation to begin during the third or fourth quarter of 2013. The preferred alternative is expected to allow for a more reliable, higher capacity secondary data center to be in place by year-end 2014. Although this will not result in relocation of the primary data center, it will significantly reduce the risks associated with loss of the primary data center.

OBSERVATION 2 –FAILOVER DATA CENTER FACILITY INFRASTRUCTURE ISSUES

We noted the existence of some issues with the facility infrastructure at the failover data center. Specifically, we noted the presence of water piping in the ceiling of the failover data center. The water piping was present because this data center was created from office space originally intended to be occupied by personnel. At the time of construction, the water sprinkler heads were removed from the piping and the piping was capped. However, the piping remained and continued to be connected to the active water based pre-action fire suppression system of the building.

Given that this fire suppression system was a pre-action type, the piping did not routinely contain water. Water is only released into the piping when an automatic detection device detects smoke or heat in the building or as a result of a valve leak. Water is only released from the piping when the heat around a sprinkler head is sufficient to melt the safety device holding the water in the piping.

Our observation also indicated that there was no water detection system in the failover data center. There is increased risk to the equipment in the failover data center from water leaking from the capped piping if the pre-action fire suppression system were to activate or a valve were to leak water.

We observed that the capacity of other facility infrastructure components, i.e. air conditioning, power distribution and UPS, for the failover data center was not sufficient to handle any additional IT equipment. Also, the current configuration of the power distribution presents risk in that its failure can impact the entire failover data center. The same exists for the air conditioning system. Colorado Springs Utilities indicated that there have been incidents in the past where equipment, and consequently processing services, has been impacted as a result of incidents caused by the malfunction of some of the failover facility's infrastructure. There is risk that both the primary and failover data centers could experience simultaneous events that would impact Colorado Springs Utilities ability to provide critical processing needs that are necessary to complete vital business functions.

AUDITOR'S RECOMMENDATION

We recommend the following:

- Colorado Springs Utilities identify and evaluate alternatives that will reduce the risk of damage to the equipment in the failover data center from water. Alternatives may include the removal of the water based fire suppression system piping, deactivation of the piping, the installation of a water detection system or relocation of the failover data center. Once a preferred solution is identified, we recommend that the alternative be implemented.
- Colorado Springs Utilities identify, evaluate and implement alternatives to reduce the risks that exist because of weaknesses in the current facility infrastructure of the failover data center.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with this recommendation and recognizes that the secondary data center is subject to risk of damage from water due to its adjacency to an abandoned water-based fire suppression system. The system is on a preventive maintenance program which requires routine inspections to ensure leaks in the piping are not occurring. As an interim measure, Colorado Springs Utilities will install a wall mounted water detection system in the secondary data center. The monitor will be connected to the centralized monitoring system to alert personnel of any water detection in the secondary data center. It is through the Security Control Center that appropriate personnel will be notified to respond on a 24/7 basis.

As noted in the response to Observation #1, Colorado Springs Utilities has also included in its capital plan for 2013 to begin relocation and expansion of its secondary data center to allow for enhanced redundancy of its systems should loss of the primary data center occur. Relocation of the secondary data center will allow for an improved design in the fire suppression system to eliminate the exposure to water-based fire suppression systems. The preferred approach and business case will be finalized in the second quarter of 2013 with implementation to begin during the third or fourth quarter of 2013.

OBSERVATION 3 – RECONCILIATION OF LISTINGS OF MEDIA STORED OFFSITE WITH OFFSITE VENDOR'S LIST OF MEDIA

During our review, we attempted to reconcile the Colorado Springs Utilities detailed listings of media stored offsite with the detailed listings of media provided by the offsite storage vendor. We noted two errors out of our small sample and suspended further testing. Although the listings were dated, they appeared to have been created at or about the same time. It did not appear to us that Colorado Springs Utilities had done a periodic reconciliation of this information. If backup media presumed to be stored offsite is not actually available, recovery of applications and data may not be accomplished in the event of an outage.

AUDITOR'S RECOMMENDATION

We recommend that Colorado Springs Utilities periodically reconcile the offsite vendor's inventory of media stored at the vendor's offsite facility with the inventory of media Colorado Springs Utilities tracks as being stored offsite. Any differences should be investigated, reported and corrected.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with this recommendation. A procedure will be developed and implemented for periodic reconciliation of the offsite vendor's inventory of media stored at the vendor's offsite facility with the inventory of media Colorado Springs Utilities tracks as being stored offsite by March 31, 2013. The reconciliation process will occur quarterly, and will be integrated into Colorado Springs Utilities' Enterprise Backup Procedures policy, QBD CCS-11058.

OBSERVATION 4 – ROUTINE INSPECTION, TESTING AND REPLACEMENT OF THE HYDROGEN SENSOR

As noted in the Commendable Practices Section of this report, Colorado Springs Utilities had installed a hydrogen sensor in the room housing the uninterruptable power supply (UPS) for the primary data center. However, we noted that there was no routine testing or inspection of this sensor to ensure that it functioned as intended. If the sensor were to fail without the appropriate staff being notified, there could be increased risk of injury to personnel and damage to equipment in the data center. This device could be providing a false sense of security because there was no way of knowing if it was functioning as intended. We also noted that the manufacturer's operating instructions recommended the sensor be replaced on a seven to ten year basis.

AUDITOR'S RECOMMENDATION

We recommend that Colorado Springs Utilities establish a process that routinely inspects and tests the operating functionality of the hydrogen sensor in the UPS room. This process should also include periodic replacement of the hydrogen sensor per the manufacturer's operating instructions.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with this recommendation. A Macurco HD-12 hydrogen sensor is used in the Uninterruptible Power Source (UPS) room for the Primary Data Center. The installation and operating manual for this device recommends testing the sensor every six months. The sensor also needs to be replaced every seven to ten years. A preventive maintenance (PM) schedule has been created for this sensor to physically inspect and test the sensor every six months. Colorado Springs Utilities will have the sensor marked with the date it was installed, and part of the PM will be to replace the sensor within the seven year period.

OBSERVATION 5 – POLICY AND PROCEDURES THAT DETAIL WHAT SHOULD OCCUR IN THE EVENT OF AN EMERGENCY SITUATION IN OR NEAR THE PRIMARY DATA CENTER

We observed that the primary data center had adequate fire detection and protection equipment. There was a Halon Abort switch and an Emergency Power-Off (EPO) switch appropriately located in the room. Personnel usually entered the data center only when it was necessary for them to complete a job function within the room. However, if a person were to be in the data center during an emergency situation, we did not observe anything that directed staff on what to do in the event of an emergency. We also did not note anything that detailed who should utilize the EPO and Halon Abort switches and when they should be used. A lack of such procedures could unnecessarily expose personnel and equipment to harm.

We noted that the emergency manual for the facility housing the data center had no indication that the building housed the data center. This manual also did not indicate a need for the coordinated shutdown of equipment located in the data center in the event of an emergency situation. The manual did not specify what personnel were responsible for the shutdown of the equipment or the details on how the shutdown of equipment was to be accomplished. The lack of specific instructions increases the risk of a loss of information and damage to the equipment if the equipment is not systematically shutdown.

We also observed that the emergency manual indicated that all employees were to receive training based on the emergency procedures detailed in the document. This manual also required all employees to receive training as part of the new hire orientation and at least annually thereafter with records of such training being maintained. We noted that this type of training was being migrated to a computer based training model, but we were unable to verify that training was occurring as required.

AUDITOR'S RECOMMENDATION

We recommend the following:

- Colorado Springs Utilities should develop and implement a policy and appropriate procedures to govern what staff should do within the data center in the event of an emergency situation. These procedures should indicate how the shutdown of equipment in the data center should be accomplished. Once developed, these procedures should be referenced in the Critical Operations Shutdown section of the emergency manual for the facility housing the data center.
- Colorado Springs Utilities should develop and implement procedures that adequately support the policy for training as detailed in the emergency manual of the facility housing the primary data center. We also recommend that such training be documented.

COLORADO SPRINGS UTILITIES RESPONSE

- Colorado Springs Utilities agrees with this recommendation. A policy and related procedures for handling emergency events within the primary data center will be developed and implemented by March 31, 2013.

- Colorado Springs Utilities will ensure that all personnel with access to the primary data center site are trained in the emergency event procedures, and that the training is documented and tracked. Initial training will be completed by May 31, 2013.

OBSERVATION 6 – FIRE SUPPRESSION TESTING ISSUES AT THE PRIMARY DATA CENTER

The documentation of the routine testing of the Halon fire suppression system in the primary data center indicated that the inspection of the cylinders holding the Halon gas were past due for testing. Management concurred that it should be determined if the cylinders should be tested and, if so, should be put on a preventative maintenance schedule. Cylinders housing Halon 1301 are to be hydrostatically tested on a periodic basis per Occupational Safety and Health Administration regulations.

We also noted that the documentation of the annual inspection of the water based fire sprinkler system had one outstanding issue. Not addressing issues found during the annual fire sprinkler inspection could result in the system not functioning as designed or intended during a fire. A malfunctioning water based fire suppression system increases the risk of damage to information and equipment in the data center.

AUDITOR'S RECOMMENDATION

We recommend that the cylinders used for the Halon fire suppression system be tested as required. We also recommend that issues identified during the annual fire sprinkler inspections be addressed and resolved.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities partially agrees with this recommendation. We concur with the requirement for annual visual inspection and five-year cycle hydro testing of the hoses in the fixed service Halon 1301 fire suppression system in accordance with National Fire Protection Association codes and standards, i.e., NFPA 12A (2009 edition), section 6.3.2. However, the following is our understanding of applicable regulation of the Halon cylinders and hydrostatic test cycles:

a. Department of Transportation (DOT) cylinders in continuous service must be given an external inspection every 5 years (inspected in place).
b. If a system discharges and/or needs to be recharged, the cylinder must have been visually inspected within the last 5 years.
c. Visual inspections are defined by Code of Federal Regulations, Title 49.
d. A hydro test of a halon cylinder in continuous use is required if the cylinder fails a visual inspection per NFPA 12A (2009 edition) section 6.2.3.

Facilities Maintenance will have a contract and/or preventive maintenance schedules in place to include annual visual inspection of the hoses, five year hydro-testing of the hoses, five-year cycle visual inspection of the Halon cylinders, and semi-annual inspection of halon-protected room enclosures at the primary data center in place no later than April 1, 2013.

The one outstanding issue noted in the last annual inspection of the water based fire sprinkler system has been addressed.

OBSERVATION 7 – POLICY AND PROCEDURES GOVERNING TRIGGERED ALARMS ON THE WATER INFILTRATION AND WATER REMOVAL SYSTEMS OF THE PRIMARY DATA CENTER

Our review indicated an absence of a policy and procedures governing what should be done in the event water infiltration sensors or the water removal system triggered alarms within the primary data center. This lack of procedures also resulted in a lack of training and understanding on what to do in case water was detected. This results in an increased risk to the equipment housed in the primary data center.

AUDITOR'S RECOMMENDATION

We recommend that Colorado Springs Utilities develop a policy and procedures to deal with activated alarms on the water infiltration and water removal systems within the primary data center. Once procedures have been established, we recommend that the appropriate personnel be trained on how to deal with such situations and that such training be documented.

COLORADO SPRINGS UTILITIES RESPONSE

Colorado Springs Utilities agrees with this recommendation. Under-floor water sensors are located in the primary data center. The center is inspected hourly by Security patrols on a 24/7 basis, especially when not occupied by data center personnel. Colorado Springs Utilities will develop a written policy and procedure to deal with activated alarms on the water infiltration and water removal systems within the primary data center. Regularly checking the condition of the water sensors will be added to the Security Operations Plan. The Facilities Management staff will take the lead in working with Information Technology staff to develop the policy and procedures, and appropriate personnel will be trained. The scheduled date to have the policy and procedures in place; the sensors added to the Security Operations monitoring system; and necessary training completed and documented is April 5, 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 and Colorado Springs Airport. 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