OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

13-16 Colorado Springs Airport Network Review

September 2013

OFFICE OF THE CITY AUDITOR
COLORADO SPRINGS, COLORADO

13-16 Colorado Springs Airport Network Review

September 2013

Purpose

The purpose of this audit was to evaluate whether the Colorado Springs Airport network promotes a secure environment that maintains the confidentiality, integrity, and availability of data and systems that either support or are supported by the network. We also reviewed management processes that included agreements between the Airport and the City's Department of Information Technology.

Highlights

We concluded that improvements were needed concerning the network controls. We identified three observations* along with one opportunity for improvement and have listed our recommendations for each in the attached report.

To accomplish our audit objectives, we reviewed policies and procedures as well as interviewed management and staff to obtain an understanding of the internal control structure around the network. We observed walk-throughs of the control operations as well as network diagrams to understand how the network is implemented, monitored, and managed. Additional information was obtained directly from vendors to establish technical specifications associated the network components. The controls identified were reviewed against the COBIT 4.1 information technology (IT) industry best practices standard for adequacy.

**Three additional observations were reported to management, which are not included in this report due to the sensitive nature of the findings. We believe publishing the details of those observations has the potential to jeopardize the security of the City and Airport networks. The Office of the City Auditor will follow-up on all observations reported to management.*

Management Response

Management was in agreement with most of the observations and recommendations. See their comments in the attached report.

Recommendations

1. Airport management should ensure the main electronics room is adequately cooled.
2. City IT management should ensure password complexity requirements are consistently enforced.
3. Airport management should formalize network performance monitoring and processes.

Opportunity for Improvement

1. Airport management should establish the level of service necessary to support business operations. Then, Airport management should work with City IT management to enhance and formalize a service level agreement for network support.

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
Public Report

Date: September 4, 2013

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

Re: 13-16 Airport Network Review

We conducted an audit of the network at the Colorado Springs Airport. The purpose of this audit was to evaluate whether the Colorado Springs Airport network promotes a secure environment that maintains the confidentiality, integrity, and availability of data and systems that either support or are supported by the network. We also reviewed management processes that included service level agreements (SLAs) between the Airport and the City's Department of Information Technology.

The audit included a review of relevant controls for the network segments utilized by the Access Control and Management System along with segments used by Airport staff.

We concluded that improvements were needed concerning the network controls. We identified three* observations and have listed our recommendations for each in the attached report. We have also noted one opportunity for improvement.

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: Steve Bach, Mayor
Laura Neumann, Chief of Staff
Dan Gallagher, Acting Director of Aviation
John McGinley, Aviation Assistant Director, Operations and Maintenance
Mark Hill, Airport Maintenance Manager, Operations and Maintenance
Tack Rice, Information Systems Analyst, Operations and Maintenance
Joe Palmer, Chief Information Officer
Jesse James, Deputy Chief Information Officer
Ken Rubel, Senior Network Engineer, Network and Systems

**Three additional observations were reported to management, which are not included in this report due to the sensitive nature of the findings. We believe publishing the details of those observations has the potential to jeopardize the security of the City and Airport networks. The Office of the City Auditor will follow-up on all observations reported to 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

Office Of The City Auditor

Colorado Springs Airport Network

REPORT DETAILS

PURPOSE AND SCOPE

The purpose of this audit was to evaluate whether the Colorado Springs Airport network promotes a secure environment that maintains the confidentiality, integrity, and availability of data and systems that either support or are supported by the network. We also reviewed management processes that included service level agreements (SLAs) between the Airport and the City's Department of Information Technology (City IT).

The scope of this review included some of the network segments utilized at the Airport. This review did not include any of the systems used at the Airport or utilized by Airport staff. There were additional network segments in use at the Airport that were not within the scope of this review. The controls tested were relevant to the following areas: short and long term plans and objectives, overall policies and procedures, SLAs between Airport and City IT, network performance monitoring, network usage logging and monitoring, logical access to network components, protection of data traversing the network, network device passwords, change management, physical access to network components, and backup and recovery.

BACKGROUND

A network consists of the wired and wireless network devices along with the transmission medium (e.g., network cabling) utilized for transporting electronic information within a localized site (e.g., within an office building or college campus).

Management of the Airport network was jointly performed by the City IT and Airport staff. City IT was responsible for the network administration, while Airport staff managed the nodes connected to the network. Additionally, many of the policies and procedures followed for the Airport network were developed and maintained by City IT because of this joint relationship. The Airport was considered an enterprise under the City and paid City IT for the services provided. Since the Airport was not receiving revenue from the City's general fund and depended only on the revenues its business operations generated, City IT was viewed as a third party service provider for this review.

The Control Objectives for Information and related Technology (COBIT) is an overarching business and management framework for governance and management of enterprise IT developed by the IT Governance Institute. COBIT provides IT professionals with a guide of globally accepted industry control best practices. The practices outlined in COBIT's framework were used in this audit to evaluate the adequacy of the controls reviewed.

CONCLUSION

We concluded improvements were needed concerning the network controls. The improvements that could strengthen controls are detailed on the pages that follow.* We also noted one opportunity for improvement.

**Three additional observations were reported to management, which are not included in this report due to the sensitive nature of the findings. We believe publishing the details of those observations has the potential to jeopardize the security of the City and Airport networks. The Office of the City Auditor will follow-up on all observations reported to management.*

OBSERVATIONS, RECOMMENDATIONS AND RESPONSES

OBSERVATION 1 – COOLING IN THE MAIN ELECTRONICS ROOM WAS NOT ADEQUATE

The area housing the core network equipment did not have adequate cooling.

All electronic equipment generates heat during its operation. Since excessive heat deteriorates these electronic components causing premature failure, it is important to have a method of dissipating the heat. As long as there are only a few devices in a small area, minimal heat build-up may occur and room temperature can be maintained allowing for effective heat convection. When the surrounding air temperature cannot be maintained at or below normal room temperature, additional cooling is necessary.

We observed that the main electronics room housing several network devices and other electronic components was insufficiently cooled. While a large fan was used to promote air circulation, the ambient room temperature was still too warm to effectively prevent electronic component deterioration. Failing network components could cause operational disruptions and could lead to unnecessary downtime in addition to the expense of repair or replacement of equipment. Airport management had previously identified this issue.

AUDITOR'S RECOMMENDATION

Airport management should ensure the main electronics room is adequately cooled.

COLORADO SPRINGS AIRPORT RESPONSE

We agree with the recommendation. The cooling system in the main electronics room has been upgraded. This issue has been resolved.

OBSERVATION 2 – PASSWORD COMPLEXITY WAS NOT BEING ENFORCED

It was identified that password complexity requirements were not configured for network device user accounts.

User account passwords should never be known by anyone other than the owner of the user account. This control prevents unauthorized personnel from gaining access to information or being able to modify systems. It also provides the ability for personnel to be held accountable for their actions. Password complexity plays a key role in preventing someone from gaining access to another user's account by guessing their password.

Guessing a password typically involves attempting to log into an account by entering the username and a commonly used password first. If unsuccessful, the next phase may include attempting to use dictionary words as the password; then progressing to attempting various combinations of letters, numbers, and special characters until the login is successful.

To make a password more difficult to guess, password complexity guidelines are usually developed. These guidelines can include such things as recommending the password not be relevant to the account owner's personal life/job/city, not containing a dictionary word, limiting repeating characters, containing more than just lower case letters, having a minimum length, etc. Many of these guidelines are typically made into requirements enforced by the system managing the usernames and passwords. These requirements force a person attempting to guess a password to make more guesses due to the password complexity, or strength. The goal is to make the password take longer to guess than the length of time before the account owner is forced to change the password.

While the City's password policy contained sufficient complexity requirements for creating strong passwords, the complexity requirements were not configured into the system managing the usernames and passwords. While the original system was configured to require strong passwords, recent upgrades had removed the requirement without informing City IT management. Without sufficient password complexity requirements, users may be creating weak passwords.

AUDITOR'S RECOMMENDATION

City IT management should ensure password complexity requirements are consistently enforced.

CITY OF COLORADO SPRINGS IT RESPONSE

We agree with the recommendation. While the password policy required complex passwords, we discovered an exception that prevented the policy from being applied at the Airport. This will be corrected by the end of June.

OBSERVATION 3 – NETWORK PERFORMANCE MONITORING WAS NOT FORMALLY REQUIRED

The Airport's network performance monitoring and relevant processes for the network segments reviewed could be enhanced.

Network performance monitoring is typically performed to ensure that the network is functioning as desired. It is typically performed by analyzing current and historical network information (i.e., bandwidth utilization and network speeds). Adequate performance monitoring would include relevant processes such as:

- A formal process to periodically maintain the production and replacement (backup) network devices.
- A formal process for the analysis of key network performance metrics supporting the business needs.
- A formal process to assess the overall performance of the networks utilizing a specifically developed monitoring method (e.g., a balanced scorecard).

Airport staff did monitor the performance of the networks. However, such monitoring was informally occurring while performing other activities, instead of a formalized process. Airport management had not established a need for such formalized processes since the current informal processes were considered sufficient and the network had not experienced any serious issues. Informal processes are more easily disregarded or forgotten, which increases the risk of business disruptions caused by network performance issues going unnoticed.

AUDITOR'S RECOMMENDATION

Airport management should formalize network performance monitoring and processes.

COLORADO SPRINGS AIRPORT RESPONSE

We agree with the recommendation. We are reviewing the current network performance monitoring procedures and processes and will formalize them.

City IT supports the Airport's response. The Airport is fully utilizing City IT's enterprise performance monitoring system, which includes all network devices. The scope of device monitoring is regularly updated by Airport staff with support from City IT. City IT will work with Airport staff to formalize the analysis of performance monitoring processes and associated data.

OPPORTUNITIES FOR IMPROVEMENT

OPPORTUNITY 1 – LACK OF FORMALIZED, AIRPORT SPECIFIC SLA FOR NETWORK SERVICES PROVIDED BY CITY IT

The Airport and City IT did not have a formalized, Airport specific service level agreement (SLA) or relevant processes in place for network services provided by City IT.

An SLA allows management to more effectively manage and utilize services, such as network services, provided by another party. It is a formal agreement between an organization and an external service provider. Among other objectives, the SLA should clearly define the roles (e.g., who is accountable for what), responsibilities (e.g., what services are being paid for), and expectations (e.g., what percentage of uptime will be provided) of the parties involved as well as how the service costs are determined. In general, an adequate network services SLA would include relevant processes such as:

- A process to mitigate the risk of the external party not being able to provide the desired level of network services.
- A process to monitor the network services provided by the external party which should, among other goals, offer assurance that services provided are meeting the business needs and that the external party is adhering to the contractual agreements.
- A process for addressing non-compliance of the external party.

Another type of agreement, an operational level agreement (OLA), is typically arranged between an IT department and other departments within the same organization. An OLA is similar to an SLA in that the roles, responsibilities, and expectations are identified; however, it is different in that the OLA is utilized for internal organization units rather than external.

At the time of our review the Airport was not receiving funding from the General Fund. It was generating its own revenue via business operations; therefore, the services provided by City IT were considered to be external services rather than internal services.

City IT had developed what they considered to be an enterprise-wide SLA; however, we determined this was actually an OLA. This OLA also provided a method for monitoring some key services. Airport management considered this OLA to be adequate for the Airport's networking service level needs. However, there was no formalized SLA in place to provide accountability of City IT in situations where Airport revenue may be lost due to insufficient network service levels being provided. Airport management had not recognized a need for a formalized SLA or the implementation of SLA relevant processes concerning network support services because they had not experienced negative issues with the services provided.

Without a formalized SLA or relevant processes, the Airport and City IT may not fully understand their responsibilities. The lack of an SLA could result in inefficient or costly network services provided as well

as potential financial losses or reputational damage due to interruption of network services. The lack of an SLA could also impact the ability of the Airport to challenge costs and the service quality provided by City IT.

AUDITOR'S RECOMMENDATION

Airport management should establish the level of service necessary to support business operations. Then, Airport management should work with City IT management to enhance and formalize an SLA for network support.

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 the 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