# Network Security Management Phases 1 and 2

## Follow-up Report

**March 2015**

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

Dennis J. Gallagher
Auditor

The **Auditor** of the City and County of Denver is independently elected by the citizens of Denver. He is responsible for examining and evaluating the operations of City agencies for the purpose of ensuring the proper and efficient use of City resources and providing other audit services and information to City Council, the Mayor and the public to improve all aspects of Denver's government. He also chairs the City's Audit Committee.

The **Audit Committee** is chaired by the Auditor and consists of seven members. The Audit Committee assists the Auditor in his oversight responsibilities of the integrity of the City's finances and operations, including the integrity of the City's financial statements. The Audit Committee is structured in a manner that ensures the independent oversight of City operations, thereby enhancing citizen confidence and avoiding any appearance of a conflict of interest.

## Audit Committee

Dennis Gallagher, Chair
Maurice Goodgaine
Leslie Mitchell
Rudolfo Payan
Robert Bishop
Jeffrey Hart
Timothy O'Brien, Vice-Chair

## Audit Management

Kip Memmott, Director, MA, CGAP, CRMA
John Carlson, Deputy Director, JD, MBA, CIA, CGAP, CRMA
Audrey Donovan, Deputy Director, CIA, CGAP, CRMA

## Audit Staff

Shannon Kuhn, IT Audit Supervisor, CISA
Nicholas Jimroglou, Lead IT Auditor, CISA
Jakki Boline, Senior IT Auditor
Karin Doughty, Senior IT Auditor, CISA

You can obtain copies of this report by contacting us at:

**Office of the Auditor**
201 West Colfax Avenue, Department 705 ◆ Denver CO, 80202
(720) 913-5000 ◆ Fax (720) 913-5247

Or download and view an electronic copy by visiting our website at:
www.denvergov.org/auditor
Report number A2010-017

# City and County of Denver

201 West Colfax Avenue, Department 705 • Denver, Colorado 80202 • 720-913-5000 •
FAX 720-913-5247 • www.denvergov.org/auditor

*Dennis J. Gallagher*
Auditor


March 16, 2015

Mr. Frank Daidone, Chief Information Officer
Technology Services
City and County of Denver
Re: Network Security Management Phases 1 and 2 Audit Follow-Up Report

Dear Mr. Daidone:

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

This report is to inform you that we have completed our follow-up effort for the Network Security Management—Phase 1 Performance Audit issued March 15, 2012, and the Network Security Management—Phase 2 Performance Audit issued July 19, 2012. Our review determined that Technology Services has implemented nine of the fourteen findings found in the audit reports.

For your reference, this report includes a Highlights page that provides background and summary information on the original audits and the completed follow-up effort. Following the Highlights page is a detailed implementation status update for each recommendation. In addition to the nine recommendations that were implemented, five recommendations were not implemented. Despite Technology Services Management's efforts, auditors determined that the risk associated with the audit team's initial findings has not been fully mitigated. As a result, the Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

This concludes audit follow-up work related to this audit. I would like to express our sincere appreciation to you and to Technology Services personnel who assisted us throughout the audit and follow-up process. If you have any questions, please feel free to contact me at 720-913-5027 or Shannon Kuhn, IT Audit Supervisor, at 720-913-5159.

Sincerely,

Kip Memmott, MA, CGAP, CRMA
Director of Audit Services

*KRM/sk*

cc: Honorable Michael Hancock, Mayor

Honorable Members of City Council
Members of Audit Committee
Ms. Cary Kennedy, Deputy Mayor, Chief Financial Officer
Ms. Janice Sinden, Chief of Staff
Mr. David P. Edinger, Chief Performance Officer
Ms. Beth Machann, Controller
Mr. Scott Martinez, City Attorney
Ms. Janna Young, City Council Executive Staff Director
Mr. L. Michael Henry, Staff Director, Board of Ethics

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

# REPORT HIGHLIGHTS

## Network Security Management Phases 1 and 2 Follow-up Report: March 2015

The Chief Information Officer has implemented nine of the fourteen recommendations made in the 2012 audit reports.

## Background

The City and County of Denver operates a large and complex data network that supports the interconnection of computers and other electronic devices used to conduct City business and to provide services to the citizenry. The Technology Services Department (Technology Services) is responsible for managing IT risks and determining which resources are necessary to mitigate those risks. The overall governance of IT is not the sole responsibility of one agency, but rather a collaborative effort between the City's top leadership, i.e., the Mayor and City Council, working closely with the leadership of the IT organization.

## Purpose

The purpose of this two-phase audit was to assess the control structure around protecting the City's data network from unauthorized access and to determine whether controls are effective in protecting network confidentiality, integrity, and availability.

## *Highlights from Original Audit*

Findings from the two phases of this audit highlighted a disturbing concern that key information security controls were not operating as a result of gaps in IT Governance. We found Technology Services was insufficiently staffed, key policies and procedures had not been developed, and there was a low process maturity environment where critical processes are ad hoc and disorganized. Accordingly, we made the following key recommendations:

1. Establish an information security governance program
2. Improve network equipment inventory controls
3. Improve controls over maintenance agreements for obsolete network equipment
4. Improve physical and logical safeguards over network equipment
5. Strengthen the resource management governance domain and improve resource monitoring and security awareness training
6. Remove network access for workstations and ports accessible to the public

## Findings at Follow-up

Technology Services has completed nine of fourteen recommendations made in the 2012 audit reports. The following areas remain in the development stage: a formal risk assessment methodology, business impact analysis, standards for disaster recovery and business continuity, information security awareness training for all users, network admission controls, and segregation of public computers and connections from the City's internal network.

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

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **Phase 1** | | | |
| **Finding 1: Information Resources Are at Risk Due to a Lack of Information Security Governance** | | | |
| **1.1** | The Chief Information Officer should establish an information security governance program with the authority to define policy and enforce standards and procedures across City agencies. | The establishment of an information security governance program began with assessing and assembling current documents into a central location. Technology Services uses the Denver One Team portal to house all IT Policies and Standards, which is accessible to all City and County of Denver employees. The governance of City technical resources is documented in detail in the policies and standards published to the City's intranet site. | **Implemented** |
| **1.2** | The Chief Information Officer should ensure the information security governance program has the full support for authority and funding from the Mayor and City Council. | The Chief Information Officer advocated for full support of this program, balanced with careful consideration of the City's projected financial situation. The 2014 budget states that the Chief Information Officer, appointed by the Mayor, is responsible for overall policy direction and management of Technology Services. The budget for 2014 allocates $392,199.00 to Compliance and Audit Services. | **Implemented** |

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **1.3** | The Technology Services Department should establish an information security governance program that is led by a person independent of operational responsibility so that the function can remain focused on directing solutions for protecting the City's information assets and network infrastructure. The components of the program should include:<br><br>• Communication and reporting to City executive management on the effectiveness and efficiency of the information security governance program according to key performance indicators. Further reporting on security incidents, information security risk trends, and any other information security risk issues that management needs to know.<br><br>• A standardized risk assessment methodology to address exceptions and provide formal notification to management with a documented and approved assumption of risk when necessary<br><br>• Business impact analyses<br><br>• Development of information security polices, standards, and procedures<br><br>• Design and execution of an employee information security awareness training program | Technology Services has partially completed pieces of the information security governance program, such as the development of information security policies, standards, and procedures; information security architectural design and review and assessment of IT projects; analysis of vulnerabilities and threats; documented incident response procedures; self-audit and compliance testing; and continuous monitoring to ensure that controls are relevant and functioning.<br><br>Although the majority of the information security program recommendations have been addressed, a few key items are still in development. Specifically, Technology Services is working towards completing the following governance program areas: standardized risk assessment methodology; business impact analysis information security awareness training program; and standards for disaster recovery and business continuity. | **Agree/Not Implemented** |

# Recommendations: Status of Implementation

| Recommendation | Auditee Action | Status |
|---|---|---|
| • Information security architectural design review and assessment of IT deployments of applications, equipment, and network configuration<br>• Vulnerability and threat analysis<br>• Developing procedures for incident response<br>• Developing standards for disaster recovery and business continuity planning<br>• Remediation strategies and projects<br>• Self-audit and compliance testing<br>• Continuous monitoring to ensure controls are still relevant and functioning as designed | | |

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **Phase 1** | | | |
| **Finding 2: Network Equipment Inventory Records Are Inaccurate Due to Missing Controls** | | | |
| **2.1** | The Technology Services Department should redesign its network equipment inventory procedures to enhance controls in four areas: | | |
| | a. Segregation of duties should be enforced to ensure that those with physical access to equipment are not responsible for updating inventory records. | The agency reviewed the job duties of the current employees and the procedures for receipt and documentation of inventory. Where possible, procedures were developed to reduce or eliminate any conflict of interest. | **Implemented** |

# Recommendations: Status of Implementation

| Recommendation | Auditee Action | Status |
|---|---|---|
| b. Access to the network equipment inventory should be restricted to a minimum number of people. File share permissions should be used to restrict access and the spreadsheet password should be eliminated. | The network equipment inventory spreadsheet and noted files share permissions restrict access to only those individuals with a need to view and update inventory equipment. | **Implemented** |
| c. A procedural checklist or some other type of transaction record should be devised to support documenting changes made to the spreadsheet. These transaction records can be used by both the people updating the records and their supervisors to ensure that all transactions are recorded accurately. The transaction records along with periodic copies of the spreadsheet should be archived for historical use. | We reviewed the procedure to ensure improvements were made to the documentation and tracking to include the procurement of an asset management application. Once a change is made to the inventory and saved, the workbook saves a backup copy of the document and records the changes made. | **Implemented** |
| d. After the preceding controls are established and tested for reliability, the entire network equipment inventory should be field verified to ensure its accuracy. This can be accomplished in phases over a period of time, perhaps up to a year. Once the entire inventory has been reconciled, only subsequent sampling of sites should be required to ensure the process is maintaining accurate records. | Once the documentation process is defined, a full inventory of network assets will be conducted. | **Agree/Not Implemented** |

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **Phase 1** | | | |
| **Finding 3: Network Equipment Maintenance Funding Allocation Procedures Are Not Documented** | | | |
| **3.1** | The Technology Services Department should design a procedure for allocating funding for network equipment maintenance to ensure that efficient allocations continue to occur in the event of personnel turnover. The procedure should identify how to determine which equipment should be included, how to determine if equipment has reached end of life, and under what circumstances maintenance should be terminated. | Technology Services developed a master source of record, which lists all assets in one document. This process includes a methodology on the maintenance to be applied to each type of equipment/license. The information is reconciled with the service provider annually to verify whether assets are properly covered. | **Implemented** |

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **Phase 2** | | | |
| **Finding 1: City Network Vulnerable to Attack or Abuse Due to Gaps in IT Governance and Low Process Maturity** | | | |
| **1.1** | The Chief Information Officer should strengthen the resource management governance domain within the Technology Services Department to ensure that adequate qualified staffing exists to perform essential security tasks. Critical security tasks should be documented and transferred to network operations personnel to ensure that essential information security controls continue to operate in the event of staff turnover. In the event that employment market conditions significantly challenge the ability to maintain staffing, the CIO should consider outsourcing network security monitoring to ensure continuous monitoring of network security controls. | The CIO strengthened IT Governance by hiring a Chief Information Security Officer, IT Governance Manager, Business Process Analyst, and three Security Network Administrators. Playbooks were created that document daily security responsibilities and critical security tasks. The playbook can be used as a desk manual and training guide for security new hires. | **Implemented** |
| **1.2** | Technology Services should revise the antivirus configurations to prevent the introduction of malware into the City network. The overall deployment of antivirus should be reviewed to prevent and detect the introduction of malware through the City's email system, and during storage, backup and restore of data files. | Technology Services implemented scanning with its new Security Information and Event Management (SIEM) system. Anti-virus scans and other alerts are monitored to ensure no (or minimal) impact to system performance. Information Security works with agencies to determine if mailboxes can be removed from shared accounts. Compensating controls have been implemented. | **Implemented** |

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **1.3** | Technology Services should also adopt technical controls to interrogate remote systems to determine if they are safe before allowing them to connect to the network. | Technology Services purchased and installed CISCO's Network access control to manage devices that connect to the network. This product verifies that anti-virus software is present and at current levels as well as ensuring patching is acceptable prior to allowing access by remote systems. | **Implemented** |
| **1.4** | The Technology Services Department should adopt network admission control technologies in order to detect and prevent the attachment of unauthorized wireless routers to the City's network. | Technology Services has not adopted admission control technologies. A plan is in place to add wireless monitoring to the QRADAR application. No implementation date was provided. | **Agree/Not Implemented** |
| **1.5** | The Technology Services Department should communicate necessary information regarding security policies to end users through periodic user security awareness training to educate agencies and users about their role in protecting the City's network, including the risks of attaching devices such as wireless routers to the network. | Technology Services hired two Security Managers who will address and develop appropriate policies. Training was planned for roll out to City employees in 2013 with a dependency on availability of funding and scheduling. The IT Governance Manager stated that City University would be used to provide the security training to users; however loading the content in City University would be time consuming. The team is now considering buying an off-the-shelf product for faster implementation. After training roll-out, end users will receive periodic education on their role in protecting the City's network, including risks of attaching devices such as wireless routers to the network. No timeframe was provided on when this would be available to users. | **Agree/Not Implemented** |

# Recommendations: Status of Implementation

| | Recommendation | Auditee Action | Status |
|---|---|---|---|
| **1.6** | The Technology Services Department should move expeditiously to segregate publicly accessible computers and connections from the City's internal network. | Technology Services will work to build a solution that maintains a secure separation between employee and public machines. The solution must be balanced with the agency's ability to properly manage and support equipment accessible to the public. No implementation date was provided.<br><br>While Technology Services did restrict access to a network monitoring application in response to this recommendation, file permissions have not been restricted and network documentation is available for public viewing. | **Agree/Not Implemented** |

# Conclusion

Technology Services has made improvements to Information Security Governance and controls by implementing more than half of the recommendations made in the Network Security Management Phases One and Two audit reports. Recommendations that are still in the process of being implemented and continue to pose a risk to the City relate to delivering security awareness training for all users, implementing a standardized risk assessment methodology, conducting a business impact analysis, performing disaster recovery and business continuity planning, and segregating publicly accessible computers and communications from the City's internal network. As a result, the Audit Services Division may revisit these risk areas in future audits to ensure appropriate corrective action is taken.

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