Final Audit Follow-Up

Status As of May 31, 2016

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Active Directory

(Report #1210 issued June 19, 2012)

Report #1616 **June 30, 2016**

Summary

This is the fourth and final follow-up on the Audit of Active Directory (report #1210 issued June 19, 2012). Thirty-one action plan steps were established to address issues identified in that audit. As of May 31, 2016, thirty (97%) of the thirty-one action plan steps have been completed or substantially completed. Applicable City staff is in the process of completing the one remaining step. Responsibility for ensuring completion of that step is turned over to management.

In audit report #1210, we noted current City policies governing the City's Active Directory were adequate, and for the most part, password controls were in place. However, we noted risks, which if realized, have the potential to negatively impact City operations. Thirty-one action plan steps were developed by management to address those risks, of which five were due for completion during this audit follow-up period.

Four of those five action plan steps were completed or substantially completed during this follow-up period. Completed steps include:

- Ensuring network authorizations are documented and can be retrieved when needed (two of three steps).
- Presenting the formal risk assessment of the City's network to the appropriate levels of City management (one step).
- Assessing risks related to systems operating outside Technology and Innovations (formerly Information System Services, or ISS) support and control (one step).

The remaining step for which actions have been initiated, but not completed relates to:

- Providing training on the new process for requesting and documenting changes in user permissions.

We appreciate the cooperation and assistance provided by staff in Technology and Innovations during this audit follow-up.

Scope, Objectives, and Methodology

We conducted this audit follow-up in accordance with the International Standards for the Professional Practice of Internal Auditing and Generally Accepted Government Auditing Standards. Those standards require we plan and perform the audit follow-up to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our follow-up audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our follow-up audit objectives.

Original Report #1210

The overall objective of our original audit (report #1210) was to review the Active Directory used to manage the City's network. Specific objectives included addressing the following questions: (1) are there adequate policies and procedures in place to effectively manage and secure the City's Active Directory, and do those policies and procedures incorporate industry best practices; (2) are the policies and procedures in place being followed; (3) is the design of the City's Active Directory implementation reasonable from a security and administrative perspective; (4) are Active Directory user accounts adequately managed; (5) are domain controllers that run Active Directory managed properly; and (6) are computer generated activity logs of network activity involving Active Directory generated, reviewed, and retained?

Overall, we concluded the policies, implementation, and management of Active Directory, as a whole, were appropriate and provided adequate security relating to the City's network. We did however

identify areas, which if addressed, would increase the security of the City's network. Those areas included:

- Increase policy compliance by deactivating user accounts that have not been used in the last 90 days.
- Eliminate the sharing of user accounts.
- Enforce password controls such as requiring periodic changing of passwords.
- Add a fourth domain to the City's network which should enhance productivity and security.
- Install updates on domain controllers in a timely manner to enhance security of the City's network.
- Conduct formal risk assessments to help ensure potential risks are considered and addressed.
- Ensure requests for changes in user network permissions are recorded and retained in a manner that allows their retrieval when needed.
- Generate, review, and retain logs of network activity to provide important information in the event network security is compromised.

Report #1616

This is our fourth and final follow-up on action plan steps provided by management in audit report #1210. The purpose of this follow-up is to report on the progress and status of efforts as of May 31, 2016, to complete the action plan steps that were developed to address the issues identified in our original audit and which had not been completed as of our last follow-up engagement (report #1603, dated January 11, 2016). To determine the status of the action plan steps, we interviewed staff and reviewed relevant documentation.

Background

In order for a computer network to operate securely there must be a mechanism in place to know who should be allowed to access the network, what they are allowed to do on the network, and what computer hardware is allowed to be part of the network. Active Directory is that mechanism for the City.

Active Directory serves as a central location for the City's network administration and security. It is responsible for authenticating and authorizing all network activity by users and computers within the City's network. It assigns and enforces security policies for the network.

Active Directory is built into the Microsoft operating system that is used on servers, but is not enabled to function on all servers. When Active Directory is enabled, that server becomes what is known as a Domain Controller, which performs the above described duties (e.g., authenticating users and computers). In the City's network there are multiple domain controllers working together to manage network activity.

The operational needs, geographic dispersal, and size of an organization are important factors to be considered when choosing the design of an organizations' Active Directory. Active Directory allows an organization to organize the elements of the network (i.e., users, computers, printers, etc.) into a hierarchical structure, similar to an organizational chart.

Active Directory implementation design is a logical organization of the City's network and is not dependent on the physical aspects of the network or the managerial organization of the City.

The significant terms relating to Active Directory design and their definitions are:

Forest: The highest organizational level of an Active Directory. Each forest is a separate installation/instance of Active Directory and can stand alone as a separate network.

Domain: A domain is a single partition of a forest and is a central collection of objects that share a directory database. This shared database contains the user accounts, computers, servers, and other hardware that make up the domain. The domain is also the Active Directory level at which users are authenticated (logged on).

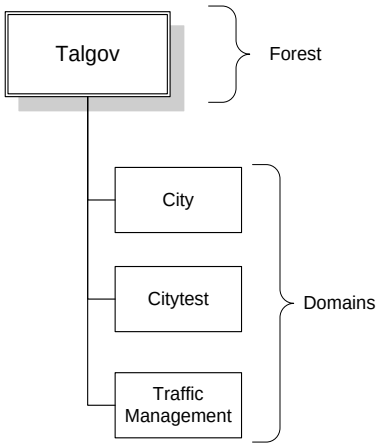
Groups: A group is a collection of users or computers. Groups allow multiple users or computers to be managed as a single unit, thereby simplifying the administration of multiple users or computers by assigning rights and permissions to the group rather than each individual user.

Users: An individual user must have an Active Directory user account to log on to the City's network. The account provides an identity for the user. Active Directory uses that identity to authenticate and grant authorization for the user to access specific networked resources (e.g., software applications and data files). User accounts are also used as service accounts for some software applications. A service account is set

up in Active Directory to allow one software application to communicate through the City's network to another software application (i.e., interface).

The City has implemented Active Directory as a single forest with multiple domains. Figure 1 shows a representation of the City's Active Directory.

Figure 1: City's Active Directory



Recent City Organizational Change: One organizational change made by the new City Manager was the restructuring and renaming of the City's Information System Services (ISS) department in January 2016. Among other things, that department was renamed Technology and Innovations and was structured such that the department now reports directly to the City Manager. Whereas the original audit report and previous follow-up reports referred to that department as "ISS," this final follow-up report now refers to that department as "Technology and Innovations, or T&I."

Previous Conditions and Current Status

In report #1210, we provided recommendations to management regarding areas that need to be addressed in Technology and Innovations (formerly ISS) relating to the City's Active Directory. Management's Action Plan consisted of 31 action plan steps. Seven of those action plan steps were reported as complete in our initial follow-up report (#1413 issued February 27, 2014), ten steps were reported as complete in our second follow-up report (#1508 issued April 20, 2015), and nine steps were reported as complete in our third follow-up report (#1603 issued January 11, 2016). Regarding the remaining five action plan steps, as of May 31, 2016, four steps were completed or substantially completed, and management has plans to complete the remaining step in the near future. Table 1 that follows shows the action plan steps and their status as determined by our follow-up process.

Table 1
Action Plan Steps from Audit Report #1210
Current Status as of May 31, 2016

Action Plan Steps	Current Status
A) Comply with APP 809 regarding the separation of development and testing environments.	
1. Evaluate the importance of establishing a fourth domain in the City's Active Directory, taking cost into consideration as well as the risks posed by the current combining of the testing and development activities in the same domain and the non-compliance with APP 809.	✓ Completed in a prior period.
2. Take appropriate actions based on the evaluation conducted in the preceding step and document the decisions made.	✓ Completed in a prior period.
B) Help ensure network authorizations are documented and can be retrieved when needed.	
1. A job code will be added to the BOSS system for changes in user account permissions.	✓ **Substantially Completed.** T&I staff developed a SharePoint form from which users may submit

	various BOSS system requests, such as changing user account permissions. Once a request is made using this SharePoint form, the requestor's department director and designated T&I management must both approve the change before it will be processed. T&I staff indicated their management review will determine whether the requestor has a legitimate business need and appropriate technological knowledge for the requested permissions. Because the BOSS request and subsequent approvals are made through a SharePoint form, the entire process is electronic which eliminates paper, yet still provides an audit trail for future reference. T&I initiated a pilot program with two City departments (Treasurer-Clerk and Human Resources) on May 27, 2016, to ensure the process works as T&I intended before making it available to all City departments. Plans are for the pilot to be completed in approximately 30 days. Accordingly, this action step is considered substantially completed.
2. Training on how changes to user account access permissions will be provided to BOSS users for the new code established in the previous action plan step.	❖ **In progress – Turned over to management to ensure completion and resolution.** As noted in the status reported for action step B1 above, T&I has developed a process whereby changes to account access permissions can be requested through SharePoint. As reported, that process is currently being vetted through a pilot program. Upon completion of the pilot program and any resulting process revisions, T&I plans to provide training on the new process to appropriate and knowledgeable staff within each City department.
3. When requests for changes to user account permissions are not completed properly in the BOSS system, they will either be corrected by T&I personnel or sent back to the requestor for correction prior to the implementation of the user account permission changes.	✓ **Substantially Completed.** As noted in the status reported for action step B1 above, T&I staff created a SharePoint form from which users may submit various BOSS requests. To help reduce the likelihood of submission errors and delays in processing of requests, T&I staff programmed the form to require proper completion of specific fields before the requestor can successfully submit the form for processing. If required fields are not properly completed, error messages will display informing the requestor of the need to correct the applicable information before submission can occur. T&I plans to include this enhancement in the process as provided to all City departments upon completion of the pilot program. Accordingly, this action step is considered substantially completed.

C) Comply with Administrative Policy and Procedure 809 and help ensure third parties granted access to the City's network understand and comply with City policies and procedures related to computers and networks.	
1. A third party compliance statement will be developed. That statement will be developed such that it will serve as acknowledgement by the party completing it that they understand and will comply with City computer and network policies.	✓ Completed in a prior period.
2. New user accounts for third parties will not be created without a completed compliance statement.	✓ Completed in a prior period.
D) Ensure third parties network access is removed in a timely manner when it is no longer needed.	
1. New user accounts set up for third parties will be configured such that they expire six months after the date they are established.	✓ Completed in a prior period.
2. All existing third party user accounts will be changed such that they expire in six months.	✓ Completed in a prior period.
3. When reviews of individual third party user accounts occur, the expiration date for those accounts will be extended for no longer than six months from the date of the review.	✓ Completed in a prior period.
E) Ensure risks to the City's Active Directory and computer network are periodically and formally reviewed and evaluated.	
1. A formal documented risk assessment of the City's network, to include Active Directory, will be conducted at least annually.	✓ Completed in a prior period.
2. The risk assessment will be presented to the CIO and the City's information technology Steering Committee.	✓ **Completed.** In our most recent follow-up report (#1603), we noted PC Solutions completed a risk assessment of the City's network, which was presented to the Chief Information Officer (CIO). Under City organizational changes enacted by the new City Manager in January 2016, the CIO position was elevated to report directly to the City Manager, thereby facilitating the CIO's ability to interact directly with the City's executive level staff and City department heads. As the City Manager believes those changes allow for the provision of more effective guidance to management as to proper utilization of the City's information system resources, the former ISS Steering Committee will be discontinued. The formal documented risk assessment was provided to the CIO as noted above. This action step is therefore considered complete.

F) Ensure system and application acquisitions are properly reviewed and approved; existing computer systems are periodically reviewed for effectiveness; and the purpose, goals, policies, and objective of T&I are reviewed by the Steering Committee.	
1. The City's information technology Steering Committee will be reactivated and meet on a quarterly basis.	✓ Completed in a prior period.
2. The Steering Committee will be informed of City activities which impact T&I or relate to information technology type system acquisitions.	✓ Completed in a prior period.
3. Guidance and approval will be sought from the Steering Committee as needed for City information technology related activities.	✓ Completed in a prior period.
4. The Steering Committee will assess risks related to systems operating outside T&I' support and control structure.	✓ **Alternative actions taken and completed.** As noted in the status reported for action step E2, the CIO position was elevated to report directly to the City Manager under City organizational changes enacted by the new City Manager in January 2016. Furthermore, because of the enhancements intended by that change, the City Manager is discontinuing the former ISS Steering Committee. Under the new organizational structure, the City's Network Security Architecture Manager within T&I will assess the risk and impact of systems operating outside the support of that department. Results of those assessments will be provided to the City's Enterprise Architecture Manager and the CIO, as well as the City Manager as needed, for managerial decision purposes. Accordingly, this step is considered complete.
G) Help ensure user accounts that have not been used within a reasonable time period are deactivated.	
1. The inactive user accounts identified in the audit will be reviewed and considered for deactivation as applicable.	✓ Completed in a prior period.
2. Quarterly a query will be made of all Active Directory user accounts which will identify all accounts that have not been utilized in the last 90 days.	✓ Completed in a prior period.
3. The user accounts identified in the preceding action plan step will be reviewed and deactivated as deemed appropriate by T&I.	✓ Completed in a prior period.

H) Help ensure user accounts are not shared by multiple individuals.	
1. User accounts in Active Directory will be reviewed for the purpose of identifying shared accounts. Shared accounts are those not assigned to a specific individual or computer service (i.e., "service accounts").	✓ Completed in a prior period.
2. T&I will review the user accounts identified in the previous step and obtain written justification from the applicable City departments as to the reasons these accounts should continue to be used.	✓ Completed in a prior period.
3. T&I will review and retain the justifications provided by the City departments.	✓ Completed in a prior period.
4. When, in T&I's judgment, the justification for the sharing of user accounts does not outweigh the risks posed by the sharing of accounts, T&I will disable the shared account. When the justification for sharing the user account does outweigh the associated risks, no action will be taken.	✓ Completed in a prior period.
I) Ensure password policies are complied with and not overridden thereby increasing the risk that user accounts may be compromised.	
1. T&I will identify all user accounts that have had password controls overridden *(i.e., accounts with passwords set to never expire).*	✓ Completed in a prior period.
2. Written justification will be obtained from applicable departments as to why those password controls should be allowed to be overridden.	✓ Completed in a prior period.
3. T&I will review and retain the justifications provided by the City departments.	✓ Completed in a prior period.
4. When in T&I's judgment, the justification for the overriding of password controls does not outweigh the risks posed by the password control overrides, T&I will remove the password override and ensure applicable password controls are enforced. When justification for password control overrides outweighs the associated risks, no action will be taken.	✓ Completed in a prior period.
J) Ensure operating system updates are installed on domain controllers in a timely manner.	
1. Updates and patches to the operating systems of the domain controllers, published by Microsoft, will be identified on a monthly basis.	✓ Completed in a prior period.
2. Within one month of the release of the updates and patches by Microsoft they will be installed on the applicable domain controllers.	✓ Completed in a prior period.

K) Ensure activity logs are generated, reviewed and retained as appropriate.	
1. Evaluate and consider the risks posed by not generating or retaining logs of the activity in Active Directory.	✓ Completed in a prior period.
2. Take appropriate actions based on the evaluation conducted pursuant to the previous step and document the decisions made.	✓ Completed in a prior period.

Table Legend:

✓ Actions completed or substantially completed

❖ Actions in progress and turned over to management to ensure completion and resolution.

Conclusion

Table 1 above shows as of May 31, 2016, Technology and Innovations (T&I) successfully completed and resolved thirty (97%) of the thirty-one action plan steps while one step is in progress with responsibility turned over to management to ensure its completion.

Four of the five action plan steps were completed during this follow-up period. Those completed steps include:

- Ensuring network authorizations are documented and can be retrieved when needed (two steps).
- Presenting the formal risk assessment of the City's network to the appropriate levels of City management (one step).
- Assessing risks related to systems operating outside T&I support and control (one step).

The remaining step for which actions have been initiated, but not completed relate to:

- Providing training on the new process for requesting and documenting changes in user permissions.

We appreciate the cooperation and assistance provided by staff in Technology and Innovations during this audit follow-up.

Appointed Official's Response

City Manager:

I am pleased to see that the Active Directory audit action plan has been substantially completed. The completion of these action items indicates that the Technology and Innovations group is continuing to improve service for the City network. The adherence to policy and the incorporation of best practices regarding the security and usability of the City technology infrastructure will ensure the most effective use of the technology resources. I would like to thank the professional dedication of the audit team in performing this analysis as well as the Technology and Innovations staff for the commitment to provide excellent service for the City of Tallahassee.

Copies of this audit follow-up #1616 or audit report #1210 may be obtained from the City Auditor's website (http://www.talgov.com/auditing/auditing-auditreports.aspx) or via request by telephone (850 / 891-8397), by FAX (850 / 891-0912), by mail or in person (Office of the City Auditor, 300 S. Adams Street, Mail Box A-22, Tallahassee, FL 32301-1731), or by e-mail (auditors@talgov.com).

Audit follow-up conducted by:
Patrick A. Cowen, CPA, CISA, CIA, Sr. IT Auditor
T. Bert Fletcher, CPA, CGMA, City Auditor