Audit Follow-Up

Status As of September 30, 2015

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

T. Bert Fletcher, CPA, CGMA
City Auditor

Active Directory

(Report #1210 issued June 19, 2012)

Report #1603 **January 11, 2016**

Summary

This is the third 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 the audit, with each step initially due for completion by September 30, 2014. As of September 30, 2015, twenty-six (84%) of the 31 action plan steps have been completed. Nine of those 26 action steps were completed during this follow-up period, while 17 action plan steps were completed in the previous follow-up periods. Actions are on-going to complete the five remaining steps.

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 to address those risks, of which 14 were due for completion during this audit follow-up period.

Nine of the 14 action plan steps were completed during this follow-up period. Those completed steps include:

- Conducting a formal risk assessment of the City's network (one step).
- Identifying and eliminating shared accounts, unless there is appropriate justification documented for keeping an account as a shared account (four steps).
- Obtaining appropriate justification to keep accounts with password controls that have been overridden, otherwise set the account so appropriate password controls are followed (three steps).
- Installing updates and patches to the domain controllers in a timelier manner (one step).

The remaining 5 steps for which actions have been initiated, but not completed relate to:

- Ensuring network authorizations are documented and can be retrieved when needed (three steps).
- Present the formal risk assessment to the Information System Services (ISS) Steering Committee (one step).
- Assessing risks related to systems operating outside ISS's support and control (one step).

We appreciate the cooperation and assistance provided by staff in Information System Services 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 #1603

This is our third follow-up on action plan steps identified in audit report #1210. The purpose of this follow-up is to report on the progress and status of efforts as of September 30, 2015, to complete the action plan steps that were initially due for completion as of September 30, 2014. 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).

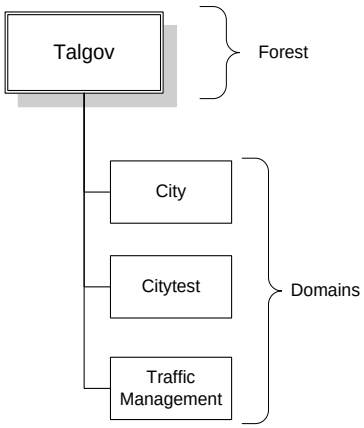
Groups: A group is a collection of users or computers. Groups allow multiple users or computers to be managed as a single unit, thereby simplifying the administration of multiple users or computers by assigning rights and permissions to the group rather than each individual user.

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



Previous Conditions and Current Status

In report #1210, we provided recommendations to management regarding areas that need to be addressed in 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), and ten steps were reported as complete in our second follow-up report (#1508 issued April 20, 2015). Regarding the remaining 14 action plan steps, as of September 30, 2015, nine were completed and actions had been initiated, but not completed, for the remaining five steps. Table 1 that follows shows the action plan steps and their status as determined by our follow-up.

Table 1
Action Plan Steps from Audit Report #1210
Initially due as of September 30, 2014, and Current Status

Action Plan Steps Initially Due as of September 30, 2014	Current Status as of September 30, 2015
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.	♦ **In Progress.** ISS stated they have been able to resolve the interface issues impacting the integration between BOSS and SharePoint, which will allow for an electronic SharePoint form to replace the manual form currently used. The SharePoint form will feed

	information into BOSS and automatically create an electronic BOSS work order ticket for ISS. Implementation of the new process is expected to begin soon and should be completed by the end of February 2016. The completion date for this action step has been amended to March 31, 2016.
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 above.	♦ **In progress.** As noted in step B1 above, ISS is developing an electronic form to replace the current manual form. ISS plans to train department users as the electronic form is being implemented. The completion date for this action step has been amended to March 31, 2016.
3. When requests for changes to user account permissions are not completed properly in the BOSS system, they will either be corrected by ISS personnel or sent back to the requestor for correction prior to the implementation of the user account permission changes.	♦ **In progress.** As noted in Step B1, ISS is developing an electronic SharePoint form to replace the current manual form. ISS stated once the revised process is in place the SharePoint form will identify errors or omissions such that key fields will only allow certain characters to be entered in those fields. For example, if the field should contain numbers, then only numeric characters will be permitted in the form. SharePoint will prevent requests from being submitted by the user unless appropriate values are entered. The completion date for this action step has been amended to March 31, 2016.
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**. ISS hired PC Solutions and Integration, Inc. (PCS) to perform a formal risk assessment of the City's network. PCS completed the assessment and issued a report to the City on August 21, 2015. The report outlined several areas where improvements can be made to enhance the City's network. ISS stated several of the recommendations have already been implemented, and plans are to complete the rest soon.
2. The risk assessment will be presented to the CIO and the ISS Steering Committee.	♦ **In progress**. As noted in step E1, PCS completed the risk assessment of the City's network. Although the report was presented to the City's Chief Information Systems Officer, ISS has not presented the report to the ISS Steering Committee. ISS stated they have recently undergone some staffing changes, and plans are for this report to be presented to the ISS Steering Committee once a new Administrator over Technology Infrastructure is hired and has an opportunity to provide additional input. Accordingly, the completion date for this action step has been amended to March 31, 2016.
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 ISS are reviewed by the ISS Steering Committee.	
1. The ISS Steering Committee will be reactivated and meet on a quarterly basis.	✓ Completed in a prior period.
2. The ISS Steering Committee will be informed of City activities which impact ISS or relate to information technology type system acquisitions.	✓ Completed in a prior period.
3. Guidance and approval will be sought from the ISS Steering Committee as needed for City information technology related activities.	✓ Completed in a prior period.
4. The ISS Steering Committee will assess risks related to systems operating outside ISS's support and control structure.	♦ **In progress.** As noted in the prior follow-up report, a Technical Advisory Group (TAG) was formed to assist the ISS Steering Committee in various activities, one of which is to perform risks assessments for City systems outside ISS's support and control. During this current follow-up engagement, ISS stated they are evaluating whether it would be feasible to acquire a software program capable of detecting systems running on City computers which will help identify those systems that are on the City's network, but outside the support and control structure of ISS. Once those systems are identified, ISS is planning to assess the associated risks and determine what action should be taken. A final completion date for this step has not been determined. We will follow up and report the status of this step in our next follow-up engagement.

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 ISS.	✓ 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.** ISS has completed their review of accounts set up in the City's Active Directory. Through this review, they determined which accounts are not assigned to a specific individual or computer service for the purpose of identifying which accounts are shared accounts, or accounts shared with more than one user.
2. ISS 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.** As stated in the reported status for step H1, ISS completed their review of accounts set up in the City's Active Directory and determined which accounts are shared accounts. After identifying the shared accounts ISS worked with departments associated with those accounts and either obtained written justification from the departments for keeping the accounts, or ISS disabled the accounts if the account was no longer needed.
3. ISS will review and retain the justifications provided by the City Departments.	✓ **Completed.** As stated in the reported status for step H1, ISS completed their review of accounts set up in the City's Active Directory and determined which accounts are shared accounts. ISS reviewed and retained written justifications from departments using shared accounts. Accounts with no appropriate justification have been disabled.
4. When, in ISS's judgment, the justification for the sharing of user accounts does not outweigh the risks posed by the sharing of accounts, ISS will disable the shared account. When the justification for sharing the user account does outweigh the associated risks, no action will be taken.	✓ **Completed.** For shared accounts identified and reviewed, ISS considered the purpose and justification, if provided, for continuation of the account. That consideration has been used by ISS to determine whether to disable or allow the shared account to remain in the City's Active Directory.
I) Ensure password policies are complied with and not overridden thereby increasing the risk that user accounts may be compromised.	
1. ISS 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.** ISS has identified departments associated with the accounts set up with passwords that never expire. After identifying which departments are responsible for these accounts, ISS either disabled the account, or obtained written justification from the department to allow those accounts to remain active and programmed with passwords that never expire.
3. ISS will review and retain the justifications provided by the City departments.	✓ **Completed.** As stated in the reported status for step I2, ISS has identified departments associated with the accounts set up with passwords that never expire. In the process of determining which accounts should be disabled and which ones should remain, ISS received, reviewed, and retained written justification from departments explaining how the account is used and why the password controls should be overridden.
4. When in ISS's judgment, the justification for the overriding of password controls does not outweigh the risks posed by the password control overrides, ISS 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.** As stated in the reported status for step I2, ISS has identified departments associated with the accounts set up with passwords that never expire. Through the process of reviewing written justification from departments associated with those accounts, ISS was able to identify and disable accounts that were no longer needed.
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.** ISS has established a process to evaluate and apply applicable updates to the Domain Controllers on at least a monthly basis. In this follow-up period, we reviewed 29 security updates released by Microsoft in August and September of 2015 that were applicable to City servers and programs. Our analysis showed ISS appropriately reviewed and applied all 29 updates in a timely manner.
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:

✓ Issue addressed and resolved.

♦ Actions initiated but not yet completed.

Conclusion

Table 1 above shows ISS successfully completed and resolved 9 of the 24 action plan steps established to address issues identified in audit report #1210 that were due during this follow-up period. Completed action plan steps include:

- Conducting a formal risk assessment of the City's network (one step).
- Identifying and eliminating shared accounts, unless there is appropriate justification documented for keeping an account as a shared account (four steps).
- Obtaining appropriate justification to keep accounts with password controls that have been overridden, otherwise set the account so appropriate password controls are followed (three steps).
- Installing updates and patches to the domain controllers in a timelier manner (one step).

Additionally, Table 1 shows the five action plan steps due for completion this follow-up period for which actions have been initiated, but not completed. Those action plan steps relate to the following:

- Ensuring network authorizations are documented and can be retrieved when needed (three steps).
- Present the formal risk assessment to the Information System Services (ISS) Steering Committee (one step).
- Assessing risks related to systems operating outside ISS's support and control (one step).

We will address ISS's success in finalizing those remaining steps in our subsequent follow-up engagement.

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

Appointed Official's Response

City Manager:

I appreciate the work done by the City Auditor on the Active Directory follow-up report. I am pleased with the progress that staff continues to make toward completion of the action items and evaluating the recommendations contained in the original audit. I am confident that all action items and recommendations will be addressed by their respective follow-up date. I would like to thank the City Auditor and DMA/ISS for their efforts in this audit and the progress made to date.

Copies of this audit follow-up #1603 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