CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

Sam M. McCall, Ph.D., CPA, CGFM, CIA, CGAP
City Auditor

HIGHLIGHTS

Highlights of City Auditor Report #1210, a report to the City Commission and City management

June 19, 2012

AUDIT OF ACTIVE DIRECTORY

We found the policies, implementation, and management of Active Directory, as a whole, appropriate and provided adequate security relating to the City's network. We did however identify issues which, if addressed, would increase the security of the City's network.

WHY THIS AUDIT WAS CONDUCTED

Active Directory is a key part of the logical security of the City's network and as such serves as the central location for network administration and security.

This audit's objectives were to:

1. Determine if policies and procedures in place are adequate to manage and secure the City's Active Directory and are those policies and procedures being followed.
2. Determine if the design of the Active Directory implementation was reasonable from a security and administrative perspective.
3. Determine if Active Directory user accounts were adequately managed.
4. Determine if domain controllers are managed properly.
5. Determine if computer generated activity logs of network activity are generated, reviewed, and retained.

This audit focused primarily on the configuration and management of the City's Active Directory and activities performed by the City Information System Services Division

WHAT WE RECOMMENDED

In the course of this audit we noted several areas relating to Active Directory where improvements could be made which would increase the security of the City's network. Several changes were recommended to improve the existing control structure. Some of the more significant recommendations include: considering the addition of a fourth domain to the City's network, improving the management of users that have been granted access to the City's network, conducting periodic formal risk assessments of the City's network, reactivating the City's ISS Steering Committee, stopping the override of user password policies, keeping domain controllers current with operating system updates and patches, and considering the generation review and retention of network activity logs.

WHAT WE CONCLUDED

The City's Information System Services department is responsible for managing the City's computer network. For the most part ISS manages the City network's Active Directory in an adequate manner. We also concluded the policies and the implementation of Active Directory were reasonable and provided adequate security over the City's computer network.

We did however identify risks that should be addressed to further increase the security of the City's network. Those risks included:

- Improvements to the management of users, specifically:
  - Deactivate user accounts that have not been used in the last 90 days,
  - Eliminate the known sharing of user accounts, and
  - Enforce established password controls
- Addition of a fourth domain to the City's network which will allow a separation of the testing and development environments.
- Updates and patches to the operating systems of domain controllers have not been installed in a timely manner which increases the risk of unauthorized access to the City's network.
- Conducting formal risk assessments would help ensure that potential risks are considered and addressed.
- Ensuring that requests for changes in user permissions are recorded, retained, and available for review when needed.
- Logs of network activity, which could provide important information in the event the security of the network is compromised, are not generated, reviewed or retained.

Recommendations were made and an action plan was developed to address each of the identified risks.

We would like to thank staff in the ISS for their assistance during this audit.

To view the full report, go to:
http://www.talgov.com/auditing/auditreports.cfm

For more information, contact us by e-mail at auditors@talgov.com or by telephone at 850/891-8397.

Active Directory

Audit Report #1210

June 19, 2012

CITY OF TALLAHASSEE
OFFICE OF THE CITY AUDITOR

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

Audit conducted by:
Dennis Sutton, CPA, CIA Senior IT Auditor
Sam M. McCall, Ph.D., CPA, CGFM, CIA, CGAP, City Auditor

Table of Contents

This page intentionally left blank.

Active Directory

Sam M. McCall, Ph.D., CPA, CGFM, CIA, CGAP
City Auditor

Report #1210 ***June 19, 2012***

Executive Summary

Overall we have concluded that policies governing the City's Active Directory were adequate, and for the most part password controls were in place. We have however noted risks, which if realized, have the potential to negatively and critically impact the operations of the City. The most serious of those risks are in the areas of domain controller management and user account management. Other issues noted include a need for greater involvement in IT governance by the ISS Steering Committee and the need for logs of Active Directory activity.

Objectives and Scope

The overall objective of this audit was to review the Active Directory that is used to manage the City's network, specifically as it relates to the security of the network.

This audit addresses 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?

Six specific questions were answered to address the audit objectives.

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:

   a) Are user accounts that should no longer have access to the City's network disabled in a timely manner?

   b) Are user accounts being shared by multiple individuals?

   c) Are the controls over user account passwords adequate based on industry best practices and are they being enforced?

5) Are domain controllers that run Active Directory managed properly?

6) Are computer generated activity logs of network activity involving Active Directory generated, reviewed and retained?

Background

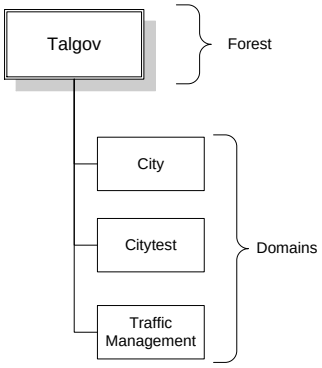
Active Directory serves as a central location for the City's network administration and security. It is responsible for authenticating and authorizing all network activity by users and computers within the City's network. Active Directory also enforces many rules as to how the network operates.

The operational needs of an organization are the determining factors to be considered when designing how Active Directory should be implemented. The significant aspects of Active Directory design include:

Forest – The highest organization level of Active Directory.

Domain – A partition of a forest. This hierarchical level contains the user accounts, computers, servers, and other hardware that makes up what is commonly known as "the network."

City's Active Directory Design



Groups – A collection of user accounts or computers. Permissions for allowed activity are defined at this hierarchical level.

Users – A user account establishes the identity of the individual accessing the computer/network. What a user is allowed to do on a network is determined by what groups they are assigned to.

The City has implemented Active Directory as a single forest with three separate domains. The forest is named Talgov and the domains are: City, Citytest, and TATMS (Traffic Management).

There are two city policies applicable to this audit of Active Directory: APP 809 "Information Systems Security" and APP 630 "Internal Control Guidelines."

APP 809 provides guidance relating to:

APP 809 and APP 630 were both identified as being applicable to this audit of Active Directory.

- Separation of production, development, and testing areas,
- Ownership of information,
- ISS responsibilities,
- Third party access to the City's network,
- Access privileges defaulting to denial when the network is not functioning properly,
- Prohibition from "browsing" the network, and
- Password controls.

APP 630 provides guidance relating to:

- Definition of internal controls,
- Conducting risk assessments, and
- Access to and accountability for resources.

City Policies

We concluded the policies we identified, as they relate to Active Directory, were adequate for the management and oversight of Active Directory. We did however note some issues with

implementation and compliance with those policies. Specifically we noted:

Contrary to policy, development and testing were conducted in the same domain.

- Development and testing activities are conducted in the same Active Directory domain (Citytest). Testing of updates and patches may negatively impact the productivity users performing development of and changes to new and current City applications/systems. We recommend ISS setup a fourth domain (Citydev) in the City's Active Directory for application/system development purposes.

Information access authorizations by information owners were not available when requested.

- Information owners are required to authorize user access to their information. ISS was unable to provide evidence for the level of access granted to users because the City's change management system (commonly known as BOSS) has not had the authorizations entered in a consistent manner. We recommend (1) ISS and information owners review the current BOSS system information access authorizations to ensure current access privileges are documented and available when needed, and (2) ISS provide additional training to City staff to ensure availability of the authorizations within BOSS.

Improvements were needed in managing third party access to the City's network.

- Compliance statements were not being completed prior to providing access to the City's network to third parties (i.e., non-city employees). In order for third parties to be granted access to the City's network, policy requires compliance statements must be completed and signed by both the information owner and the third party. A compliance statement acknowledges the third party understands and will comply with City policies and procedures relating to computers and networks. We recommend ISS no longer grant third party access to the City's network without completed compliance statements.

- Reviews of third party access privileges were not conducted as required. Policy requires semiannual review of access privileges for third party users. We recommend ISS configure third party user accounts such that they expire every six months to help ensure reviews are conducted as required and that third party user accounts do not remain valid for extended periods of time after they are no longer needed. We also recommend ISS review the existing user accounts and deactivate existing third party user accounts that have not been recently used.

Formal documented risk assessments of Active Directory would be highly beneficial.

- We noted ISS continually and informally assess the risks facing Active Directory; we also noted however that formal documented risk assessments would be highly beneficial for management when managing the City's Active Directory. As such we recommend ISS consider periodic, documented formal risk assessments to assist in ensuring that applicable risks are considered.

Active Directory Design

The design of an Active Directory should be based on the size, the geographic dispersal, the security needs, and the resources available for administration. The City has implemented Active Directory as a single forest with three domains.

We concluded that implementing Active Directory as a single forest was a reasonable design choice based on the above identified factors.

The current design of Active Directory includes three domains; City (production), Citytest (testing and development), and TATMS (traffic management).

We recommend the establishment of a fourth domain to separate development and testing activities.

As previously noted, application development and testing are both conducted in the Citytest domain. Per policy these activities should be in separate environments. Additionally, it is a best practice for them to be separated so that problems caused by testing do not negatively impact the productivity of the users performing development activities. We recommend establishment of a fourth domain within the Talgov forest for development activities.

Systems/Applications Outside Active Directory

In the course of this audit it came to our attention that there are several IT type systems that are operating outside the control of Active Directory and are not part of ISS support/control structure.

We noted several IT type systems that were operated outside the support/control structure of ISS.

Examples of those type systems include the SCADA (Supervisory Controls and Data Acquisition) system for the Electric Utility, the SCADA system for the TP Smith Wastewater plant in the Underground Utility, multiple systems at the airport, and the City's smart metering system. Per ISS, when these systems were proposed and approved it was not clear that consideration was given to how the changes or additions to the City's IT systems would impact ISS's ability to support those systems (with existing ISS resources). Those systems were not within the scope of this audit.

We recommend the ISS Steering Committee be reactivated.

The ISS Steering Committee is responsible for citywide IT governance, specifically reviewing the purpose, goals, policies, and objectives of ISS, reviewing proposals for acquisitions of new systems, reviewing existing computer systems for effectiveness, and recommending projects for implementation. We noted the ISS Steering Committee has not met since March of 2007 and as such has not discharged its responsibilities in relation to the above identified systems, all of which have been implemented since the committee last met. We recommend the ISS Steering Committee be reactivated and that they make an assessment of the risks related to those systems operating outside ISS's support and control structure.

User Accounts

User accounts are the mechanism used to determine who can log onto the City's network and what information can be accessed. While reviewing user account activity we noted issues relating to how those accounts were used. Specifically we noted user accounts that had not been used within a reasonable time, user accounts that were being shared by multiple employees, two password controls that had not been enforced, and password controls that were overridden for certain accounts.

We noted numerous user accounts that had not been used within a reasonable time period.

We noted numerous user accounts that had not been used within a reasonable period of time, those type user accounts are commonly known as inactive accounts. The risks from inactive user accounts are that if an account is compromised it may not be detected for a considerable period of time and if an account is not used regularly that password is not being periodically changed thus increasing the chances that it could be compromised. In the course of our testing we identified 143 user accounts that were active but had not been used within the last 90 days. We also noted 226 user accounts that were active but had never been logged into since they were created. We recommend ISS review user accounts that are inactive and deactivate those accounts which are not needed.

We recommend ISS review and deactivate inactive user accounts that are not needed.

Several user accounts that were shared by multiple individuals were noted in our examination of user accounts.

Our testing of user accounts also showed there were user accounts being shared by multiple employees. The risks from users sharing accounts are that monitoring activity to a specific user is more difficult and passwords are often either not changed or they are written down so that all employees sharing the account know the password. An example of user account sharing we noted were the dispatchers and call takers for public safety. We recommend ISS review user accounts and identify all accounts not assigned to a specific individual. With those accounts identified we recommend ISS have the applicable user department justify why shared accounts should be allowed to continue. ISS should then weigh the increased risk from shared accounts against the justifications provided. For the instances where the justification outweighs the risk, no changes should be made. However for the accounts where the justification does not outweigh the risk, we recommend ISS work with the impacted departments and develop alternatives to account sharing.

We recommend ISS find alternatives to user account sharing.

Password usage is the most common means of securing user accounts. In our examination of the controls relating to password usage we noted that most password best practices were in place and being utilized. Those best practices included: a password control relating to password history was in place to prevent previous passwords from being reused, passwords were set to expire after a set time period forcing the need for them to be periodically changed, a minimum password length was required, and user accounts were disabled after passwords were entered incorrectly several times. We also noted two best practice password controls that were being implemented through a third party application rather than through Active Directory. The first was a requirement for a minimum password age; this prevents a user from making several password changes in quick succession and then returning to a previous password. The second is a minimum level of password complexity, which requires the use of a mixture of alpha and numeric characters which greatly increases the difficulty for attempts at password guessing attacks by "hackers".

We identified two password best practices that were not implemented.

We recommend ISS impose a minimum password age requirement and include password complexity in Active Directory.

Finally, in our review of password controls we noted user accounts that had their password controls overridden to where they were different than the controls imposed on most other accounts. We noted numerous instances where user accounts had been set to have their passwords never expire. We recommend ISS identify all instances where user accounts have been set to never expire and require applicable departments justify, in writing, why the accounts should be allowed to continue with passwords that never expire. ISS should then review those justifications and change the password settings when the justification does not justify the increased risk from having accounts with passwords that do not expire.

Instances of password controls being overridden were noted.

Domain Controllers

A domain controller is a computer server that is used for running Active Directory and is arguably the most important piece of hardware in a computer network.

The physical security of domain controllers is important because if one were to be physically compromised it would be possible for a hacker to extract and use passwords (hashes), install viruses, add user and administrator accounts, and add computer scripts that are run every time the domain controller is restarted. Any of which could completely compromise the network. As such, we examined the security of the domain controllers and noted they were kept in locked and secured rooms.

We identified 25 updates for the domain controllers that had not yet been installed.

Our examination of domain controllers included determining if they are being kept current with updates and patches published by Microsoft, the makers of Active Directory. We noted that during the fourth quarter of calendar year 2011 there were 18 security updates and 7 non-security updates applicable to the domain controllers used by the City and that none of those updates had been installed as of 4/14/2012. When we inquired as to why the updates had not been installed it was communicated to us that installing the updates could potentially negatively impact operations by causing the network to "crash" and they should be thoroughly tested prior to installation. However, per ISS the resources for that testing were not available. Therefore the updates have not been installed. Due to the importance of domain controllers we recommend the resources for testing updates be identified and allocated to ensure updates and patches are kept up to date on the City's domain controllers.

We recommend ISS identify the resources needed to ensure domain controllers are kept current with updates.

Activity Logs

Logs of Active Directory activity are not being generated.

We noted in this audit that logging of Active Directory activity was not occurring as recommended by best practices. Logging is the system generation of a record of the events that occur in a computer system. Logs can be used to provide; alerts to suspicious activity, tracking of unauthorized activities, assistance in the recovery of servers, assistance in investigations, and information needed for legal proceedings. We asked why logging of Active Directory was not occurring and were told that sufficient resources were not available for logging. Specifically it was communicated that there was not adequate data storage capacity and there were not enough resources for reviewing logs if they were generated. Inadequate resources for logging is a common issue in many organizations. In response, broad based best practices have been developed to help ensure resources are used as efficiently as possible. The best practices fall into areas that include determining: what needs to be logged, how long the logs should be retained, how often and in what detail logs need to be reviewed, and how the logs should be secured.

We recommend ISS reconsider the decision to not log the activity within Active Directory.

We recommended ISS reconsider the decision to not log Active Directory activities and consider implementing a logging plan that will use resources as efficiently as possible.

Active Directory

Sam M. McCall, Ph.D, CPA, CGFM, CIA, CGAP
City Auditor

Report #1210 *June 19, 2012*

Objectives

The overall objective of this audit was to review the Active Directory used within the City's computer network.

The overall objective of this audit was to review the Active Directory that is used to manage the City's network, specifically as it relates to the security of the network. That review consisted of answering the following questions:

Six specific questions were answered to address the audit objectives.

1) Are 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:

   a. Are network user accounts that should no longer have access to the City's network disabled in a timely manner?

   b. Are user accounts being shared by multiple individuals?

   c. Are the controls over user account passwords adequate based on industry best practices and are they being enforced?

5) Are domain controllers that run Active Directory managed properly?

6) Are computer generated activity logs of network activity involving Active Directory generated, reviewed and retained?

Scope and Methodology

In this audit we reviewed and evaluated the implementation of Active Directory as it relates to the logical security of the City's computer network. Our audit of the City's network was limited to the City domain and did not include the City's test domain or the domain devoted to the Tallahassee Advanced Traffic Management System (domains will be described in the background section of this report), except as they relate to the design of the Active Directory. Additionally, we did not include an evaluation of the adequacy of the hardware used in the City's network for supporting operation of Active Directory.

Applicable audit procedures were conducted to meet the stated audit objectives. Those procedures included conducting interviews of knowledgeable personnel, inspecting and analyzing various guidance, records, and reports. Specific procedures included:

Our procedures included interviewing knowledgeable staff and analyzing applicable industry guidance and various City records and reports.

- Identifying and evaluating City policies and procedures that address or impact the design and management of the City's Active Directory,
- Identifying and reviewing industry materials relating to the design, configuration, and management of an Active Directory,
- Identifying and learning how to use software tools designed to obtain and analyze information in Active Directory,
- Extracting, querying, and reviewing Active Directory data, and
- Interviewing staff involved in the administration and management of Active Directory.

We conducted this audit 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 to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Active Directory Overview

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 is the central location for the City's network administration and security.

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 a component of the operating system published by Microsoft and used by the City on certain servers.

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 and performs the above described duties (i.e., authenticating users). In the City's network there are multiple domain controls and they work together to manage network activity.

Active Directory Design

Operational needs, geographic dispersal, and size of the organization must be considered when designing an Active Directory installation.

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 tree like 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.

A domain is a partition of a network and is the Active Directory level at which users log in.

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 makes up the domain. The domain is also the Active Directory level at which users are authenticated (logged on).

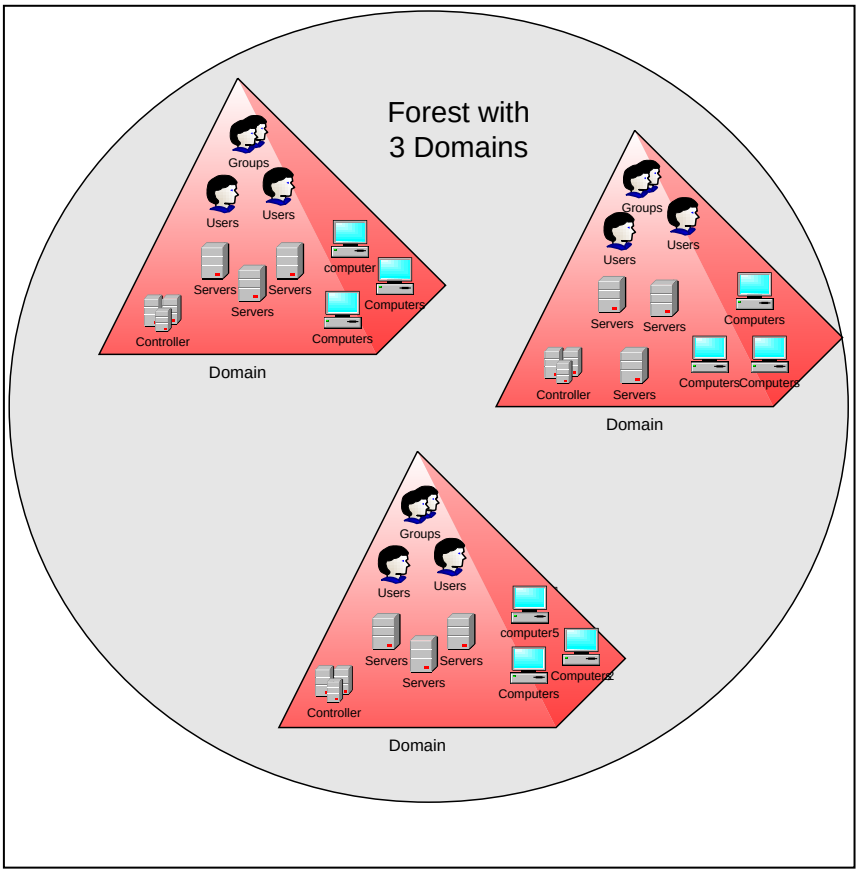
Groups - A group is a collection of users or computers. Groups allow multiple users or computers to be managed as a single unit, thereby simplifying the administration of multiple users or computers by assigning rights and permissions to the group rather than each individually.

Users - A user requires an Active Directory user account to log on to a computer or to a domain. The account establishes an identity for the user; Active Directory then uses this identity to authenticate the user and to grant him or her authorization to access specific domain resources. User accounts can also be used as service accounts for some applications. That is, a service can be configured to log on (authenticate) as a user account, and it is then granted access to specific network resources through that user account.

An illustration of how users, computers, and servers are part of a domain and domains are part of a forest is shown in Illustration 1 below:

The City has implemented Active Directory as a single forest with three separate domains.

Illustration 1
Representation of Forest with 3 Domains

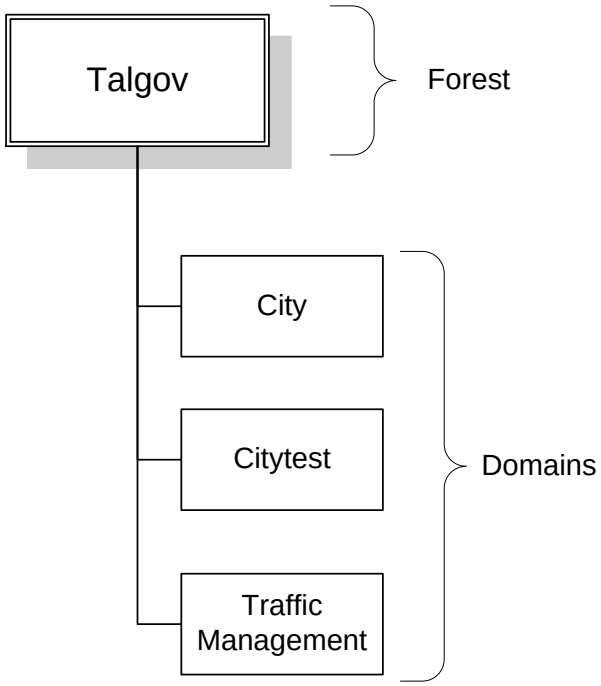


As stated earlier, Active Directory is a Microsoft product that is built into the operating system used on servers and has been developed such that it is scalable and can be implemented in a wide variety of design configurations. For example, it has the flexibility to be used for networks ranging from an international company's worldwide network to a small single location organization's network. The major differences between those two

implementations of Active Directory relate to the number and complexity of forests and domains included in the organization.

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

Figure 1
City's Active Directory



The design of the City's Active Directory will be discussed further in a subsequent section of this report.

City's Active Directory History

Active Directory was first implemented in the City in 2001.

The City first implemented Active Directory in 2001. This was approximately one year after Microsoft released Windows 2000, which was the first release of Active Directory. Prior to implementing Windows 2000 (an older Microsoft server operating system) and Active Directory the City used Windows NT to control the network.

Policies relevant to the City's Active Directory

There are two City policies that have a direct bearing on Active Directory.

There are two City policies applicable to the audit of Active Directory. The first is Administrative Policy #809 "Information Systems Security Procedures" (APP 809). The second policy is Administrative Policy #630 "Internal Control Guidelines" (APP 630). Both of those policies as they relate to Active Directory are described below.

APP 809 – Information Systems Security Procedures

Active Directory plays a key role in enforcing several provisions of APP 809 – Information Systems Security Procedures.

APP 809 states, "It is the policy of the City of Tallahassee that a standard method for information systems security be established." The policy does not specifically mention Active Directory as part of that security method for information systems security; however, our audit showed that it is one of the key tools for implementing the provisions of the policy. Additionally, we noted the policy provides direction on the implementation and administration of Active Directory. Therefore, Active Directory is used to enforce aspects of the policy and the policy provides guidance on how Active Directory should be implemented.

Specific provisions of the policy applicable to implementation of Active Directory and its administration include:

There should be a separation between production, development and testing environments.

809.5.1.1.3 - Separation between production, development, and test systems: This section of the policy states there should be a separation between production, development and testing environments. The purpose for this requirement is to ensure the security of the applications the City relies on for day to day operations (production environments) while the other environments (development and testing) can maximize productivity with fewer security restrictions.

An "owner" of information within the City's production environment must be designated.

809.5.1.2.1 - Information Security Ownership: The policy requires that an "owner" of information in the City's production environment be designated and that the owner has certain responsibilities. As it relates to Active Directory, this means that information owners must:

- Approve information oriented access control privileges for specific job profiles;
- Approve other information oriented access control privileges which do not fall under the existing specific job profiles;
- Review and correct reports that indicate the job profiles currently having access to their information; and
- Approve all new and different uses of their information.

In summary, this means that information owners must designate, review, and approve who has access to their information.

809.5.1.2.5 - Information Systems Services: This part of the policy designates ISS as having responsibility for "creating workable information security compromises which take into consideration the needs of the users and owners of City information." Additionally this part of the policy makes ISS responsible for managing access control administration activities and monitoring the security of the City information systems.

Access to the City's network and information must be approved in writing by the "owner" of that information.

809.5.3.1.3 - Third Party Access to City Internal Networks: This provision of the policy requires that both the information owner and project manager must agree in writing to such access before such access will be granted. Privileges for such third party access must be strictly limited to only the information clearly needed to achieve the predefined business objectives. Additionally, these access

privileges must be reviewed every six months by the project manager to determine whether access needs to be continued.

809.5.3.1.7 - Default to Denial: This section of the policy requires that when a City computer or network access control system is not functioning properly is must default to denial of privileges to users.

809.5.3.1.21 Browsing: This part of the policy prohibits users from browsing through City computer systems or networks. For example, curious searching for interesting files and/or programs on the network is prohibited.

809.5.9.1.4.1.2 - Passwords: These sections of the policy require that users choose passwords that are difficult to guess and are not identical or substantially similar to previous passwords. Additionally, the policy requires (1) all computers connected to the City's network to use passwords to log on, (2) the initial password issued to users must be changed after the first time it is used, and (3) user accounts must be disabled after consecutive failed logon attempts to prevent password guessing attacks.

APP 630 - Internal Control Guidelines

City policy APP 630 defines internal controls and has implication for the management of Active Directory.

APP 630 states, "It is the policy of the City to establish and maintain an internal control structure designed to ensure that reliable data are obtained, maintained, and fairly disclosed in reports." APP 630 does not specifically refer to Active Directory as part of the internal control structure for the City or for the City's information systems. However, APP 630 has implications in the operation and management of the City's Active Directory which is a key part of the internal control structure of the City's network. The applicable parts of the policy and their implication to Active Directory are summarized below.

630.06 - Definition and objectives of Internal Control: "Internal control is a process effected by an entities board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations."

As a key part of the City's computer network's internal controls, Active Directory facilitates each of the above categories by restricting access to the network (when appropriate) and limiting what users are allowed to do on the network.

Risk assessments help identify where efforts may need to be increased to mitigate potential risks.

630.09.II - Risk Assessments: This portion of the policy states that risk assessments are mechanisms with which a department can determine the relative potential for irregularities or non-compliance in programs and functions. It goes on to state that risk assessments should be performed periodically. As it relates to Active Directory, we interpret this to mean that periodically ISS should be considering risks related to network access and user permissions within the network as well as evaluating the risks relating to the configuration/design of the Active Directory.

630.09.III.2 – Access to and Accountability for Resources: This section of the policy identifies that access to resources and records should be:

Access to resources should be limited to those with authorization to access them.

- Limited to authorized individuals
- Designed to assign and maintain accountability for the custody and use of resources
- Periodically compared to recorded accountability.

Active Directory is the key part of the City's network for controlling access to resources and records on the City's network.

Overall Summary

Overall, based on our audit, we concluded the City's implementation and management of Active Directory was appropriate and provided adequate security relating to accessing the City's computer network.

Overall, we found the design used in Active Directory was based on a reasonable balancing of security and administrative requirements.

We found the design used for the City's implementation of Active Directory was reasonable and provided a balance between administrative requirements and security. However, we also found that the addition of a fourth domain to the City Active Directory forest could improve both security and productivity.

We found that the policies in place for the administration of the Active Directory were adequate for the management of Active Directory and that for the most part the administration of Active Directory was in compliance with those policies. However, we did note some instances of non-compliance.

We found there were numerous user accounts that had not been used within a reasonable time frame (i.e., 90 days) and could be considered inactive but had not been deactivated within Active Directory. We also noted several instances of user accounts being shared by multiple individuals. Finally, it came to our attention that certain password controls which were in place for most user accounts had been overridden for some user accounts.

We found that the domain controllers that run Active Directory were adequately secured. However, we noted a significant issue relating to the installation of updates to operating systems of the domain controllers.

We reviewed the usage of activity logs within Active Directory.

Finally, we reviewed the usage of activity logs in relation to active Directory. In that review we noted issues with the use of generation review and retention of activity logs relating to Active Directory.

For issues identified in the course of this audit, we have made recommendations to assist in addressing the risks posed by those issues.

City Policies

Our first audit objective was to determine whether current City policies that impact Active Directory provide for the establishment of a reasonable and appropriate internal control structure around and within Active Directory. In addition to consideration of the adequacy of the policies we evaluated the City's implementation of Active Directory for compliance with those policies. Applicable industry guidance was identified, reviewed, and considered in connection with that evaluation.

Our first objective was to evaluate the adequacy of and test for compliance with policies that impact the administration of Active Directory.

Adequacy of Policies

Our audit evaluation considered each of the separate reserve components.

Policies have an important role in the management of the City's Active Directory. They provide guidance to employees as to what is expected from them in relation to their duties and Active Directory.

Our review of the policies of the City showed that there was no policy that specifically identified, referenced, or directed the usage of Active Directory. We did not take issue with this lack of direct referencing of Active Directory as a policy deficiency because Active Directory is a tool used to enforce policies. For example, Active Directory is the tool that is used to help enforce the policy that users of the City's network not "browse" through the network *(APP 809.5.3.1.21).*

Our review of APP 809 and APP 630 showed that the policies were adequate for the oversight and management of Active Directory.

We did note there were policies APP 809 (Information Systems Security Procedures) and APP 630 (Internal Control Guidelines) in place which had an impact on the management of Active Directory.

Our review of the above identified policies showed that the policies were adequate for the oversight and management of the City's Active Directory.

Compliance with Current Policies

Active Directory is a key tool used in enforcing the main City policies relating to network security. The following paragraphs highlight the key security policy provisions that are enforced through Active Directory and our conclusion/comments as to compliance with the policies.

APP 809 – Information Systems Security Procedures

APP 809.5.1.1.3 – Separation of Production, Testing, and Development Environments

This portion of the policy requires that there be a separation between production, testing, and development environments. This separation is also a best practice in the IT industry as it helps prevent operational downtime due to issues with developing and/or testing changes to applications. Our examination of the design of Active Directory showed partial policy compliance. As described in the background section of this report, a separate domain (Citytest) has been created for testing of application changes. We noted however, the Citytest domain is also used for application development, which is in violation of this policy. Development is an important ongoing process that helps ensure a continuous improvement in City operations. Interruption of application development would negatively impact several City departments if interrupted by a failure caused by the testing of things such as

We noted that testing and development were not in separate environments as required by policy and best practices.

operating system updates and hardware changes. We recommend that ISS consider adding a fourth domain to the City's Active Directory for development purposes. This issue will be subsequently discussed in our review of the design of the Active Directory implementation.

APP 809.5.1.2.1 – Information Security Ownership

Policy requires that information owners authorize access to the information for which they have responsibility.

In order to ensure that information/data created and stored within the City's network is managed and controlled, this section of the City's information security policy has mandated that an "owner" of the data be designated. The policy stipulates that an information owner does not actually own the data (the data belongs to the City) rather they have responsibility for determining the usage of that data and authorizing who has access to the data. As it relates to Active Directory, ownership of data means that owners must notify ISS as to changes in access authorization to the data for which they have responsibility. The current process for owners to approve access to their data is for the owner (or designee) to complete a form or "ticket" within the City's change management system (commonly known as BOSS).

The authorizations for access to the City network are not retained in a manner that allows them to be retrieved when needed.

As part of our testing of user access we attempted to obtain copies of the BOSS tickets where the access was authorized by the information owner. However, due to the manner in which those authorizations are recorded in the BOSS system, we were unable to extract the necessary information. We next requested ISS's (the department responsible for managing the BOSS system) assistance in obtaining those BOSS tickets. We were told the requests for network/data access authorization within the BOSS system were not always made in a consistent manner by information owners. This inconsistency makes the retrieval of the authorizations very difficult and therefore not practical to be retrieved when needed.

Based on this understanding of the way in which authorizations are recorded in the BOSS system, we have concluded that while there may have been owner approval for access to data when the access to the data was granted, it was not practical to retrieve that approval when needed.

Absent the applicable BOSS tickets, neither ISS nor the information owners are able to demonstrate that only authorized individuals have been given permission to access the information owner's data. We recommend that ISS and information owners review the current BOSS system to ensure authorized access granted is documented and readily available for review upon request.

We further recommend ISS provide additional training to City staff that uses the BOSS system, and make changes to the BOSS system to ensure availability of information within the BOSS system which will allow those authorizations to be retrieved when needed.

APP 809.5.1.2.5 – Information System Services

Balancing information system security with usability is an important concept that must always be considered when designing and implementing IT systems and applications. This section of the policy designates ISS as having responsibility for creating "workable information security compromises" which take into consideration the needs of the users and owners of City information. The policy also assigns responsibility for controlling access to the City's information systems to ISS.

Figure 2
Illustration of the Balance of Security vs. Usability

In our review of the design of the City's Active Directory (See Active Directory Design section of this report) we concluded that ISS has taken a reasonable approach when considering the security aspects of the Active Directory design and the administrative overhead requirements of the various Active Directory design options. During the course of this audit we also noted ISS is controlling access to the information systems network through the use of Active Directory as required by the policy. We conclude that ISS has complied with this section of the information security policy through its implementation and management of Active Directory.

APP 809.5.3.1.3, .4, and .5 – Third Party Access to City Internal Networks

Access to the City's network and information is required, from time to time, by various third parties (e.g., vendors and law enforcement agencies) that serve or assist the City. These sections of the policy delineate the requirements for allowing those third parties access to the City's network and information. The policy requires that information owners (described in APP 809.5.1.2.1 above) complete a "compliance statement" to authorize network access by third parties. The compliance statement must also be signed by the third party and serves as the third party's acknowledgement that they

understand and agree to abide by the City's policies and procedures related to computers and networks. Additionally, the policy requires a review of those third party access privileges every six months to evaluate the need for that access privilege to be extended.

Compliance statements were not prepared prior to granting access to third parties as required by policy.

Our review showed that the compliance statements were not being completed by the information owners nor were there acknowledgments by the third parties documenting that they understood and would comply with City policies and procedures related to computers and networks. The review also showed that the six month reviews were not occurring as required. For example, we noted several third party vendors which had been granted user access (one as far back as 2007) and never used that access, yet the user account was still active as of January 2012.

We recommend ISS no longer grant access to the City's network to third parties without completed compliance forms.

We recommend ISS comply with the above policy and no longer grant access to third parties without the information owner (or designee) completing, and the third party signing, the required compliance statement. Additionally, we recommend that when ISS sets-up user accounts for third parties they configure those accounts such that they "expire" and are no longer active after six months. This will help ensure that (1) third party vendor accounts do not remain inactive for extended periods of time and (2) reviews of the user access occur as required by the policy. Finally, we recommend ISS review the existing user accounts and identify all third party user accounts that have been granted access to the City's network and consult with the applicable City departments to determine if that access is still necessary. For the third party user accounts that are still deemed necessary, ISS should require the information owners to complete and have the third party sign compliance forms.

APP 809.5.3.1.7 – Default to denial

The policy requires the City's network deny network access when the access control system is not functioning properly. One of the main functions of Active Directory is to control access to the City's network. In our review of the functionality of Active Directory, we noted that it is designed such that the network cannot be used without Active Directory functioning properly. As such, we have concluded that the City's usage of Active Directory satisfies this policy requirement.

APP 809.5.3.1.21 – Browsing

Active Directory is configured such that it assists in enforcing the policy against "browsing" the City network.

Searching through or browsing of the City's network is prohibited by this section of the policy. The policy gave the example of "curious searching through the network" as being prohibited. Active Directory helps enforce this policy by limiting the access of users to only the parts of the network for which they have specifically been granted access. However, there are many files and folder on the City's network which have been designated as "common" and are accessible to anyone that can log onto the network. Therefore, Active Directory does not completely ensure compliance with this policy requirement, but it does serve as a tool to help enforce the policy.

APP 809.5.9.1.4.1, .2 – Password System Set-up

Passwords are important because they help prevent unauthorized access to important information by serving as a mechanism for verifying the individual attempting to access the information is who they claim to be. These sections of the policy address password usage and requirements. Table 1 (shown below) illustrates the policy requirement related to passwords and our conclusions as to compliance with the policy.

Table 1
Password Policy Compliance

Policy Requirement	Auditor Comments/Conclusions
Employees must choose passwords that are hard to guess.	✓ The City's Active Directory has been configured such that there are minimum password requirements, for example the minimum password length is 8 characters and the password must be periodically changed. These requirements are enforced through a third party application.
Employees must not construct passwords that are identical or substantially similar to previous passwords.	o This is a good requirement for password security. However, there is no mechanism within Active Directory to enforce the prohibition from using similar passwords. However, we noted Active Directory was configured such that passwords cannot be immediately reused.
All computers permanently or intermittently connected to the City's network must have password access controls.	✓ Active Directory requires a password for a user to connect to the City's network. However, that requirement can be disabled by an administrator over Active Directory. Our examination of user accounts did not show any instances of user accounts that have had the requirement for password usage disabled.
Initial passwords issued to new users or issued when the user requests a password reset must be valid for only the first logon and need to be changed by the user once used.	✓ Our review of Active Directory showed that there is the ability to force password change on next logon. This functionality must be set by the administrator that reset the password for the user. We were informed forcing password change is standard practice for ISS.
To prevent password guessing attacks, the number of consecutive failed logon attempts must be limited. After 3 unsuccessful logon attempts the user account must be disabled until reset by an administrator or for no less than 3 minutes.	✓ We noted in the course of our examination of Active Directory, it is configured such that a user account is disabled for 3 minutes after 5 unsuccessful logon attempts. While the policy stipulates the user account should be disabled after 3 attempts, the current configuration of disabling accounts after 5 attempts does not materially change the security of the network; as such we do not take exception with the deviation from the policy.
✓ Addressed and enforced through Active Directory o This policy provision cannot be enforced through Active Directory	

APP 630 Internal Controls

The City's internal control policy, APP 630, is intended to define internal controls and establish guidelines for establishing adequate internal controls over operations.

In our review of the policy for applicability to Active Directory and ISS's compliance with the applicable provisions of the policy we noted the following:

APP 630.06 - Definition of and Objectives of Internal Controls

ISS recognizes the important role Active Directory plays in the internal control structure of the City's network.

We discussed with ISS staff the role of Active Directory in network security, and based on those discussions it was clear ISS has recognized the key role that Active Directory plays in the system of internal controls over the City's network.

APP 630.09.II – Risk Assessments

Periodic risk assessments are a key part of ensuring the internal controls are still helping mitigate the risks the controls are designed to address. During the course of this audit we inquired as to how ISS assessed the risks of the City's network as a whole and specifically those risks relating to Active Directory. We were informed that while there was no formal risk assessment process they did continually, but informally, evaluate the risk environment and risks faced by the City's network and by Active Directory. While this is a good practice that should be continued, we believe it would be highly beneficial to periodically conduct and document formal risk assessments of the City's network. As such, we recommend ISS periodically conduct a formal risk analysis of the City's network that includes Active Directory and how it can be used to help mitigate the risks the City's network faces as well as assess the risks that are specific to Active Directory.

We recommend ISS periodically conduct formal risk assessments of Active Directory.

APP 630.09.III.2 – Access to and Accountability for Resources

The basic concept behind restricting access to resources is to reduce the risk of unauthorized use or loss of those resources. From a City network standpoint there is a large amount of sensitive information and other resources the City needs to protect within the computers and servers of the City. Active Directory is a key component of the internal controls over restricting access to those resources in the City's network. Our testing showed that Active Directory has been designed and managed with network security as a prime consideration.

Policy Summary

Our review of City policies showed the existing policies relating to Active Directory are adequate to govern the functioning of the Active Directory. We did however note some aspects of City operations that could be changed and if so would both improve compliance with policies and improve the security of the City's network as it relates to Active Directory. For example, a fourth domain should be added to the City's network for software development purposes, the usage of City's BOSS system should be better standardized to document approvals and facilitate information retrieval, City departments and ISS should better comply with policies related to granting third party vendors access to the City's network, and a periodic formal assessment of the risks facing the City's network and Active Directory should be conducted.

Active Directory Design

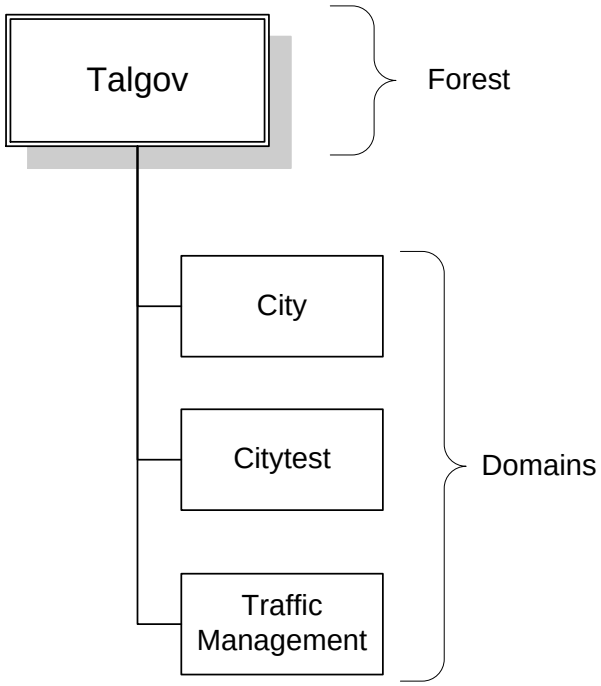
As briefly discussed in the background section of this report there are many factors to consider when developing the design of Active Directory. Those factors include the size of the organization, the geographic dispersal of the organization, the resources available for

administration, and the needs of the various parts of the organization for autonomy.

There are many factors to be considered when choosing a design for an Active Directory implementation.

As previously stated in the background section of this report, the City has implemented Active Directory as a single forest with three domains.

Figure 2
City's Active Directory



Single forest design choice implications

The City's Active Directory has been implemented with a single forest named "Talgov." The City's decision to implement Active Directory as a single forest vs. multiple forests involved a balancing of administrative requirements and security needs.

The City's Active Directory is implemented as a single forest design.

From a strictly security standpoint, using multiple forests in an Active Directory implementation is more secure than using a single forest. For example, a multiple forest implementation of Active Directory would provide the ability to create a strict separation

between parts of the organization thus preventing the compromise of the security of one part of the network to potentially compromise the entire network. Multiple forests are most often used when there is a need for:

- Autonomy: With the use of multiple forests each forest is managed independently, enabling each forest to have separate and different business rules. Often this is driven by organizational structure or operational requirements. For example, the City's utilities could be separated from the rest of the City's network as a separate forest. This would allow the utilities to operate (from a network perspective) autonomously from the remainder of the City.
- Isolation: Each forest in a multiple forest implementation can operate independently of the other forests. Usually this level of separation within a network is required because of legal or operational requirements. For example, if there was a legal requirement that law enforcement applications and databases must be completely separate from the rest of the City's network this separation could be achieved through the use of a second forest.

The disadvantage of utilizing multiple forests is that each forest must be managed separately. This means that separate domains, user lists, permissions, and directories must be developed and maintained. Adding a second forest to an Active Directory implementation effectively doubles the administrative requirements needed when compared to a single forest implementation.

The decision to implement Active Directory as a single forest is a reasonable balance of security and administrative requirements.

The City's decision to use a single forest Active Directory design as opposed to implementing multiple forests is a compromise between the administrative requirements vs. administrative resource availability.

Three Domains in the City's Active Directory

A domain is a logical division (or partition) of a forest in Active Directory. The City has implemented Active Directory with three separate domains. Those domains are:

City

The City domain is the domain where City operations are conducted.

This domain is used for the majority of the City's operations and is the domain that most employees utilize on a day to day basis. This is the domain of the City's Active Directory where we conducted our testing of user permissions and passwords.

Citytest

The Citytest domain serves as the environment for both testing and development.

This domain allows the City to conduct testing of new applications and updates to applications without potentially negatively impacting the day to day operations of the City. Dividing the testing of applications and updates into a domain separate from the operational domain (City) is a best practice recommended by most IT professionals, and is required by policy (APP 809.5.1.1.3, described above). We noted however, in addition to testing, application development takes place in the City's test domain (as briefly described in the policy section of this report).

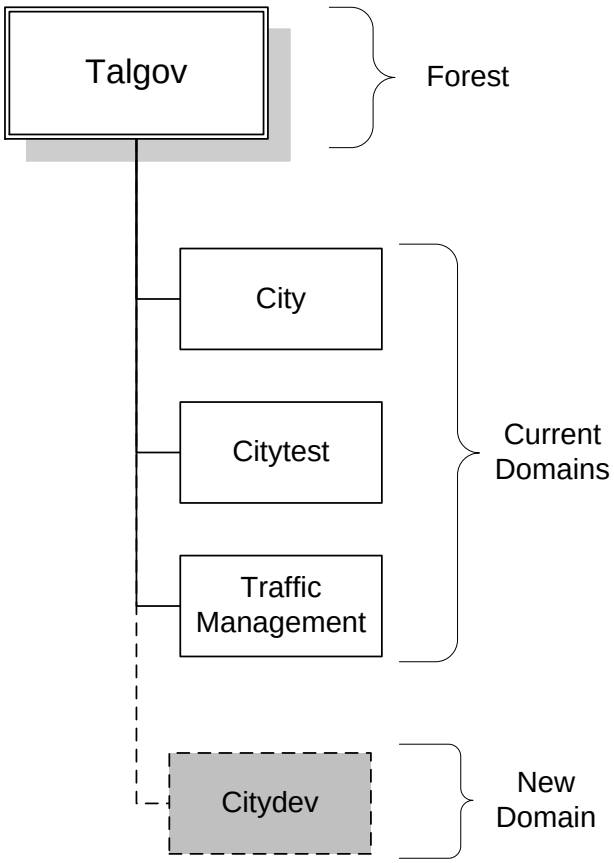
We recommend ISS consider the deployment of a fourth domain for development purposes.

Application development is an important part of the ongoing daily operations of the City. A simple example of application development is the implementation of new budget or expense codes within the City's PeopleSoft Financials application. These new codes must be added and then tested/reviewed/approved to ensure they have been coded and implemented correctly prior to their use in the City's live production environment (i.e., the City domain). It is a best practice that the separation of testing and development be accomplished through dividing the two into separate domains. This separation will prevent problems caused by testing from impacting the productivity of the employees that work on the development of applications used by the City. We recommend that management consider implementing a new domain for application and system development purposes within the Talgov forest of City's Active Directory. Figure 3 below illustrates the potential design of the

City's Active Directory with a separate domain for application development.

Figure 3

Potential Active Directory Design With a Fourth Domain



TATMS

This domain is for the Tallahassee Advanced Traffic Management System. Per management, TATMS has been separated into a separate domain due to legal requirements from the Federal Government.

Systems/Applications not included in Active Directory

While conducting this audit it came to our attention that there are several IT systems / applications that are not operating within the control of the City's Active Directory. In essence this means they operate outside the City's network. Additionally they are not under ISS's support/control structure; therefore either (1) third party vendors are being retained for support of these systems, or (2) the applicable departments are hiring their own IT professionals to support the systems; either of which may not be the most efficient use of City resources.

Examples of systems outside ISS support/control include the SCADA (Supervisory Control and Data Acquisition) system for the Electric Utility, the SCADA system for the Thomas P. Smith Wastewater Plant in the Underground Utility, multiple systems at the City's airport, and the City's smart metering system. When we inquired of management as to why these systems have been allowed to develop and function outside the support/control of ISS we were told the systems were approved and developed with senior management and City Commission approval. However, it was not clear that consideration was given to how the changes or additions to the City's IT systems would impact ISS's ability to support those systems with existing resources. Those systems were not within the scope of this audit.

The purpose of the ISS Steering Committee is to provide management guidance to the organized efforts of properly utilizing the City's information system resources. The ISS Steering Committee is specifically charged with responsibility for:

- Reviewing the purpose, goals, policies, and objectives of ISS;
- Reviewing proposals for new system acquisitions;

- Reviewing existing computer systems for effectiveness; and
- Recommending projects for implementation.

The above responsibilities are part of the IT governance process for the City. The ISS Steering Committee has not met since March of 2007. We recommend the ISS Steering Committee be reactivated and that they make an assessment of risks related to systems operating outside ISS's support and controls structure.

User Accounts

A user account is the mechanism in Active Directory that is used to determine who can log into the City's network and what information can be accessed. For the City, employees must have a user name and password to log on to the network.

Inactive Accounts

User accounts that have not been logged into recently are considered inactive accounts.

User accounts which have not been logged into within a reasonable time frame (i.e., 90 days) are often called inactive accounts. These types of accounts pose an increased risk to the security of the network. The risk from inactive accounts is twofold. The first risk is that the passwords assigned to the accounts are not periodically changed thereby increasing the chances that the passwords for the accounts could be compromised thus giving an unauthorized individual access to the City's network. The second risk is that if a user account was compromised the unauthorized access would go undetected for an extended period of time because the authorized account user is not using the account and would not notice the unusual activity. Therefore, for network security purposes, it is a best practice for user accounts which have not been used recently to be deactivated.

We noted 143 user accounts that are inactive and an additional 226 that have never been used.

As part of our testing of user accounts we examined all user accounts in the City domain in order to determine the last time the accounts were logged onto the network. In the course of our examination we noted 143 (of the approximately 3,200 active user accounts in Active Directory) had been previously used but not logged into within the last 90 days. Those user accounts consisted of, but were not limited to, accounts for regular employees, third parties (i.e., vendors) that had been given access to the City's network, test user accounts, and individuals from external law enforcement agencies. In addition to the 143 inactive but previously used accounts we identified, we noted an additional 226 user accounts that were also active but had never been logged into since they were created. Those user accounts consisted primarily of employees and third party vendors.

We recommend ISS review and disable inactive accounts as applicable.

Due to the number of inactive accounts we noted in our testing, and the risks those accounts pose to the security of the City's network, we recommend that ISS review the user accounts with the applicable City departments to which those accounts grant access and deactivate those accounts which are not needed. Additionally, as previously recommended in the policy section of this report, we recommend that third party user accounts be configured such that they expire and automatically deactivate after six months.

Shared User Account

Best practices suggest that user accounts not be shared.

Shared user accounts are user accounts that are used by more than one user. It is a generally accepted best practice that user accounts should not be shared as it renders the security over those accounts less effective.

There are two specific risks associated with sharing of user accounts. The first risk is that having two or more individuals

sharing a single account makes monitoring activity to a specific user more difficult. The risk is increased when one realizes that there is the possibility of multiple logons to the same account at the same time. The sharing of accounts also can lead to lessened care for security by users as the users do not feel the same level of accountability for the activity that occurs on the shared account. The second risk relates to passwords. With multiple individuals using the same account, periodic changing of passwords is more difficult as all the users utilizing the account must be told the new password. This leads to the writing down of passwords or the elimination of the requirement for periodic password changes, either of which is a security weakness. (Not requiring periodic changing of passwords was noted in our testing/review of passwords, discussed in a subsequent section of this report.)

Recognizing risks relating to shared accounts, there are instances where sharing of passwords is reasonable. For example, sharing of a single guest account by multiple individuals with limited and tightly controlled access privileges (i.e., internet access only) is an instance where sharing of accounts could be considered reasonable.

We noted several instances of accounts being shared among multiple employees.

In our examination of user accounts, we noted several instances of accounts that were shared. For example, we noted that the dispatchers for the public safety departments have shared accounts. When we inquired of ISS as to why this occurred, we were told that it was done at the direction of the police department (who houses the public safety dispatch operations of the City) because communicating password changes was too difficult with multiple users working non-stop across three shifts per day. We also noted shared accounts used for things such as, but not limited to, training, the setup of new computers, testing, and various other operational needs.

We recommend ISS identify all shared accounts and have user departments justify, in writing, the sharing of those accounts.

While, as noted, there are sometimes instances where shared accounts are reasonable those instances should be limited to every extent possible. We recommend that ISS review the user accounts within Active Directory and identify all accounts that are not assigned to a specific individual. Once identified, we recommend that ISS notify the applicable departments and require those departments to submit written justification as to why the shared accounts should be allowed to continue to be used. If ISS, in their professional judgment, determines the justification for users sharing accounts outweighs the increased risks associated with sharing accounts, no changes to the current situation should be made. However, if ISS does not believe there is adequate justification ISS should assist the departments in developing an alternative to allowing the sharing of accounts.

Password policies

Passwords are the most common means of securing user accounts.

The use of passwords is the most common means of securing computer user accounts. While there are other means of ensuring that only the authorized individual utilizes a computer account (i.e., biometrics) the use of passwords is often adequate from a security standpoint and is a fairly inexpensive security mechanism to implement and maintain.

Password security is dependent on users keeping their passwords secure and the strength of the password.

The strength of the security provided by the use of passwords is dependent on two things; (1) users keeping their passwords secure, and (2) the strength of the passwords used. Best practices relating to passwords from a user standpoint includes:

- Users to never share their passwords,
- Users to never write down their passwords, and
- Users to change passwords immediately if they suspect their password may have been compromised.

From a computer systems standpoint, best practices relating to passwords call for:

- Enforcing password history – set policy such that passwords cannot be reused within a certain time period,
- Password age – Set policies such that passwords cannot be changed within a certain time period after they have already been changed (i.e., must wait a certain number of days before password can be changed a second time),
- Password expiration – passwords expire after a set time period and must be changed,
- Minimum password complexity standards – require that passwords have a minimum level of complexity, such as use of mixed upper and lower case letters, use of numbers, and use of special characters (i.e., $, &, @, etc.),
- Minimum password length – only allow the use of passwords that exceed a minimum number of characters, and
- Account lockout – user accounts are "locked" after a set number of incorrect logon attempts.

As part of this audit we could not test the passwords being used for compliance with the above requirement because the passwords are encrypted. We did however examine the password requirement settings within Active Directory that govern the passwords users are allowed to choose when setting their passwords. To do this we reviewed the password controls implemented within the City's Active Directory and compared those controls to the above noted best practices and the policy requirements of APP 809.5.9.4.1 (discussed in the policy section of this report).

We noted that neither a minimum password age nor a minimum level of password complexity were enforced.

In our review of password controls within Active Directory we noted that password policies (controls) had been implemented. We noted the following:

- ✓ The previous five passwords were remembered and could not be reused for the next five password changes.
- ✓ A minimum password age was not enforced through Active Directory; however it was enforced through a third party application. This prevents users from immediately rotating through five "temporary" passwords and back to the

previous password used, thus allowing the user to use the same password continuously and circumvent the password history requirement,

- ✓ Passwords were set to expire within a reasonable timeframe thus forcing users to change their passwords,
- ✓ A minimum level of password complexity is enforced through a third party application,
- ✓ The best practice for minimum password length is 8 characters and the City's Active Directory password length policy met or exceeded this standard, and
- ✓ After a number of unsuccessful logon attempts Active Directory locks out the user account for a set time period.

Our examination of password policies within Active Directory showed two areas where password controls could be strengthened. We recommend ISS review the password policies enforced within Active Directory and change those policies to require a minimum password age as well as an increased level of password complexity.

Password policy override

It was noted that there were instances where password controls were overridden to allow accounts with passwords that never expire.

Active Directory permits the established password policy to be overridden at the individual user account level. In our testing of user accounts we noted there were instances where the "global" password policies had been changed at the individual user account level.

Specifically we noted there were numerous instances where passwords were set to never expire. In most instances the accounts with no password expiration were accounts that were shared user accounts (e.g., the public safety dispatchers as previously described). However, we also noted instances where passwords for third party (vendor) user accounts were also not set to expire after a set time period.

User accounts with passwords that do not expire increases the risk that those accounts could be compromised.

User accounts with passwords that do not expire, thereby eliminating the need to periodically change the password, increases the risk the accounts could have their passwords compromised and the accounts will remain compromised and undetected for an extended period of time. We recommend ISS review all instances where user account passwords have been set to never expire and remove the never expire designation from as many user accounts as possible.

Domain Controllers

A domain controller is a computer server that is used for running Active Directory. Domain controllers are arguably the most important pieces of hardware in a computer network because they are responsible for:

A domain controller is the server that runs Active Directory.

- authenticating all activities on the network,
- managing the security database that holds all the policies and permissions for all objects in the network, and
- replicating changes made to the security database to all other domain controllers on the network.

Typically there are multiple domain controllers within a computer network and they all share the task of controlling the network. Due to their key role in managing a network, domain controllers should be one of the most protected pieces of hardware on the network. Threats to a domain controller include attempts to:

- Gain access to the security database on the domain controllers,
- Copy the security database (for examination off-line),
- Change permissions and rights of existing users, and
- Add or change computers allowed in the network so rouge computers can access the network.

Each of these threats could lead to a complete compromise of the security of a network. To help minimize the threats to the domain controllers there are several measures that should be taken to help increase their security. Those measures include physically securing

the domain controllers, keeping the operating systems current with updates from Microsoft, and not allowing applications other than Active Directory to run on the domain controllers.

Physical Security

Physical access to the domain controllers should be limited to the greatest extent possible. If a domain controller were to be physically compromised it is possible for a "hacker" to:

- extract and use encrypted passwords (hashes),
- install malicious computer code (e.g. viruses),
- add user and administrator accounts, and/or
- create or modify logon scripts (computer code that runs every time the server is restarted).

We noted no exceptions with the physical security over domain controllers.

Any of these four items could completely compromise a computer network.

As part of this audit we examined the physical security of the domain controllers that are part of the City's network. In that examination we noted the domain controllers were kept in secured computer rooms which limited physical access adequately.

Operating system updates

Installing updates (or patching) is important for all computer operating systems and applications. This is especially true for domain controllers due to the unique threats they face.

Keeping the operating system of domain controllers up to date with updates and patches is important.

However, keeping the domain controllers up to date with updates and patches is a challenging and time consuming task. Every month, Microsoft publishes many updates and patches for its' products; all of which must be reviewed to identify those that are applicable to the City's domain controllers. Once the appropriate updates and patches are identified, they should be tested for compatibility and potential negative impacts to the network and

other applications using the network prior to their installation. Additionally, when updating and patching domain controllers there is the risk that a problem with an update could cause the entire network to no longer function properly.

Our testing showed the domain controllers were in excess of 90 days out of date with updates and patches.

As part of our testing of the City's domain controllers we reviewed the updates/patches that had been installed. Our review showed the domain controllers were considerably out of date with respect to updates and patches. For example, we noted that during the fourth quarter of calendar year 2011 Microsoft published 18 security updates and 7 non-security updates that were applicable to the City's domain controllers. Of those 25 updates, none had been installed as of 4/14/2012.

When we brought this to the attention of ISS and inquired as to the reasons for the delays in installing the updates/patches we were informed that they were aware of the situation. We were also told that they recognized the importance of keeping all City systems current with updates and patches (not just domain controllers). Management stated the reason updates and patches were out of date was due to a lack of resources for testing prior to installation and concerns that installation without adequate testing could cause a severe negative impact to City operations. Management also stated that because there is ongoing development within the Citytest domain there were fears that installing updates or patches without other testing could cause that domain to "crash" which would have a serious negative impact on several City departments.

The fear of negatively impacting operations by testing updates and patches for domain controllers in the Citytest domain further supports our previous recommendation of developing a fourth domain for development purposes.

We recommend the resources to update and patch the domain controllers be identified and allocated to help ensure their security.

Due to the importance and the potential for catastrophic failure of the City's network if the domain controllers were compromised, we recommend the resources for testing updates be identified and allocated to ensure updates and patches are kept up to date on the City's domain controllers.

Activity logs

Logging of network activities is an important part of a sound security posture.

According to the National Institute of Standards and Technology Guide to General Server Security, logging is a cornerstone of a sound security posture. In a network security environment a log is a system generated record of the events (activities) that occur in a network and are often the only record of those activities. Logs can and typically are used for creating an audit trail of the actions that occur in a network and can provide:

- alerts to suspicious activities that require further investigation,
- tracking of an unauthorized network intruder's activities,
- assistance in the recovery of a server from a failure of that server,
- assistance in investigations, and
- information that could be needed for a legal proceeding.

A challenge of managing network logging activities is balancing the resources available for generating, maintaining, and reviewing logs with the large amount of data that can be logged.

Activity logs of Active Directory are not being generated, reviewed or maintained.

With Active Directory's key role in authenticating activities in the network, logging of Active Directory is an important tool for detecting issues with network activity. As such, we inquired of ISS as to the logging of network activities that is conducted in Active Directory. When we inquired of ISS as to what logs are generated, reviewed, and maintained we were told that logging of Active Directory does not occur due to a lack of resources. It was reported to us that the lack of resources was in two areas (1) limited data

storage capacity for logs, and (2) limited resources for reviewing the logs if they were generated.

The issue of inadequate resources for logging is a common issue that is faced by many organizations that maintain computer networks. In response, several broad based best practices have been developed within the IT industry. Logging best practices fall into four general areas:

- Log generation – Log generation relates to determining what activities will and can be logged with available resources (i.e., will only security related activities be logged?).
- Log retention – Log retention deals with determining where and how the logs should be retained, how long the logs should be retained, and if or how should log data be archived.
- Log analysis – Log analysis involves determining what data that has been logged should be periodically reviewed in detail, what log data analysis should be automated (i.e., automatic reports that summarize log data), what logged activities should create automatic alerts for immediate review, and what logged data should be retained solely in the event it may be needed for investigative purposes in the future.
- Log security – Log security is ensuring that the logs are secured in such a manner that they cannot be altered or deleted to "cover the tracks" of unauthorized activities the logs are recording.

Management should reconsider the decision to not log activity in Active Directory.

We recommend management reconsider the decision to not log Active Directory activities and consider implementing a logging plan that evaluates the best practice areas identified above to help ensure resources are used as efficiently as possible.

Conclusion

With the exception of the areas listed below we found the policies, implementation, and management of Active Directory, as a whole, appropriate and provided adequate security relating to the City's network.

Overall, we found the implementation and management of Active Directory to be appropriate and provide adequate security for the City's network.

Areas, which if addressed, would increase the security of the City's network include:

- increasing policy compliance by deactivating user accounts that have not been used in the last 90 days,
- eliminating the sharing of user accounts,
- enforcing password controls such as requiring periodic changing of passwords,
- ensuring that requests for changes in user network permissions are recorded and retained in a manner that allows their retrieval when needed,
- adding a fourth domain to the City's network which should enhance productivity and security,
- updates have not been installed on domain controllers in a timely manner which creates a security risk to the City's network, and
- logs of network activity are not being generated, reviewed or retained which could provide important information in the event the security of the network is compromised.

For issues we identified audit recommendations were made.

For each of those areas we identified in which improvements could be implemented, we made recommendations that would reduce the risks in those areas.

We would like to thank staff in the ISS for their assistance during this audit.

Appointed Official's Response

City Manager:

The City Auditor's Office has conducted a thorough and detailed audit of the City's Active Directory environment maintained by the Information Systems Services Division (ISS). Providing technology solutions and protecting our most valuable asset - our data, is of the highest priority to the ISS division. I am extremely pleased with the cooperation demonstrated by Mr. McCall's team and staff during this audit. The audit findings and the recommended improvements will result in measurable benefits to this government. The action items identified in this report will ensure that our internal controls and City policies continue to be strictly adhered to in the future. I would like to thank the Auditor's Office as well as ISS for their hard work on this audit.

This page intentionally left blank.

Appendix A – Action Plan

Action Steps		Responsible Employee	Target Date
A. Objective:	**To 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.		Terry Baker	4/1/2013
2. Take appropriate actions based on the evaluation conducted in step A.1. above and document the decisions made.		Sabrina Holloman	9/30/2013
B. Objective:	**To help ensure network authorizations documented and can be retrieved when needed**		
1. A job code will be added to the BOSS system for changes in user account permissions.		Jim Van Riper	4/1/2013
2. Training on how changes to user account access permissions will be provided to BOSS users for the new code established in step B.1. above.		Jim Van Riper	5/1/2013
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.		Terry Baker	5/1/2013
C. Objective:	**To comply with APP 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.		Terry Baker	6/1/2013
2. New user accounts for third parties will not be created without a completed compliance statement.		Terry Baker	6/1/2013

Action Steps		Responsible Employee	Target Date
D. Objective:	**To 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 established.		Terry Baker	10/1/2013
2. All existing third party user accounts will be changed such that they expire in six months.		Terry Baker	10/1/2013
3. When reviews of individual third party user accounts occur, the expiration date for the account will be extended for no longer than six months from the date of the review.		Terry Baker	10/1/2013
E. Objective:	**To ensure risks to the City's Active Directory and computer network are periodically and formally reviewed evaluated**		
1. A formal documented risk assessment of the City's network, to include Active Directory, will be conducted at least annually.		Terry Baker	10/1/2013
2. The risk assessment will be presented to the CIO and ISS Steering Committee for review.		Terry Baker	10/1/2013
F. Objective:	**To ensure system and application acquisitions are properly reviewed and approved; existing computer systems are periodically reviewed for effectiveness; 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.		Sabrina Holloman	4/1/2013
2. The ISS Steering Committee will be informed of City activities which impact ISS or relate to information technology type system acquisitions.		Sabrina Holloman	9/30/2013
3. Guidance and approval will be sought from the ISS Steering Committee as needed for City information technology related activities.		Sabrina Holloman	9/30/2013
4. The ISS Steering Committee will assess risks related to systems operating outside ISS's support and control structure.		Sabrina Holloman	9/30/2013

G. Objective:	**To 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.		Terry Baker	6/1/2013
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.		Terry Baker	6/1/2013
3. The user accounts identified in step G.2. above will be reviewed and deactivated as deemed appropriate by ISS.		Terry Baker	6/1/2013
H. Objective:	**To help ensure user accounts are not shared by multiple individuals**		
1. User accounts in Active Directory will be reviewed for the purpose of identifying accounts that are not assigned to a specific individual for computer service (i.e., "service accounts").		Terry Baker	9/30/2013
2. ISS will review the user accounts identified in step H.1. above and obtain written justification from the applicable City departments as to the reasons these accounts should be allowed to be continued to be used.		Terry Baker	9/30/2013
3. ISS will review and retain the justifications provided by the City departments.		Terry Baker	9/30/2013
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.		Terry Baker	9/30/2013
I. Objective:	**To ensure password policies are complied with and not overridden thereby increasing the risk that the user accounts may be compromised**		
1. ISS will identify all user accounts that have had password controls overridden.		Terry Baker	10/30/2013
2. Written justification will be obtained from applicable departments as to why those password controls should be allowed to continue to be overridden.		Terry Baker	10/30/2013
3. ISS will review and retain the justifications provided by the City departments.		Terry Baker	10/30/2013

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 the justification for password control overrides does outweigh the associated risks no action will be taken.	Terry Baker	3/31/2014
J. Objective:	**To 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.	Terry Baker	12/30/2013
2. Within one month of the release of the updates and patches by Microsoft they will be installed on the applicable domain controllers.	Terry Baker	3/31/2014
K. Objective:	**To 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.	Terry Baker	4/30/2013
2. Take appropriate actions based on the evaluation conducted in step K.1. above and document the decisions made.	Sabrina Holloman	5/31/2013