



CITY OF SAN ANTONIO

P. O. BOX 839966
SAN ANTONIO TEXAS 78283-3966

May 13, 2010

Julián Castro
Mayor

Jennifer V. Ramos
Councilwoman, District 3

Ray Lopez
Councilman, District 6

Elisa Chan
Councilwoman, District 9

Mary Alice P. Cisneros
Councilwoman, District 1

Philip A. Cortez
Councilman, District 4

Justin Rodriguez
Councilman, District 7

John G. Clamp
Councilman, District 10

Ivy R. Taylor
Councilwoman, District 2

David Medina, Jr.
Councilman, District 5

W. Reed Williams
Councilman, District 8

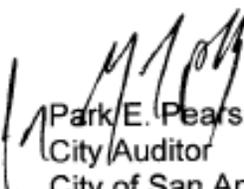
Mayor and Council Members:

SUBJECT: Information Technology Services Department Information Security Program Audit Report

We are pleased to send you the audit report of the Information Technology Services Department. This audit began in July 2009 and concluded with an exit meeting with department management in March 2010. Management's verbatim response is included in Appendix E of the report. The Information Technology Services Department should be commended for its cooperation and assistance during this audit.

The Office of the City Auditor is available to discuss this report with you individually at your convenience.

Respectfully submitted,


Park E. Pearson, CPA
City Auditor
City of San Antonio

Distribution:

Sheryl L. Sculley, City Manager
Pat DiGiovanni, Deputy City Manager
Richard Varn, Chief Information Officer
Hugh Miller, Chief Technology Officer/ Director
Michael D. Bernard, City Attorney
Leticia M. Vacek, City Clerk
Robbie Greenblum, Chief of Staff, Office of the Mayor
Jaime Castillo, Communications Director, Office of the Mayor
Frances A. Gonzalez, Assistant to the Mayor, Office of the Mayor
Catherine J. Hernandez, Interim Executive Assistant to the City Manager
Stanley Blend, Audit Committee Member
Manuel Long, Audit Committee Member

CITY OF SAN ANTONIO
OFFICE OF THE CITY AUDITOR



Audit of the Information Technology Services Department
Information Security Program

Project No. AU09-009

May 13, 2010

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an audit of the Information Security Program implemented by the Information Technology Services Department (ITSD). Moreover, this is the first in a series of audits we will perform over the next few years to assist ITSD by evaluating information technology (IT) general controls which apply to all or a large segment of the City's computer applications (see **Appendix C** on page 10 for our tentative IT audit schedule). The audit objective and conclusion follow:

Has ITSD established and implemented an effective entity-wide Information Security Program?

We determined that ITSD management initiated an entity-wide Information Security Program. However, although some IT component systems may be secure, the entity-wide security program is in its infancy and certain internal controls have either not been developed or have been developed but not fully implemented. Our review of ITSD's draft of the plan for information security, which is the foundation of its Information Security Program, showed that it contains all key security elements as recommended by the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM).

We observed that:

- Although drafted, ITSD has not completed its plan for the IT Security Program (ITSP).
- ITSD currently has only one full-time dedicated IT security person.
- There is no formal process in place to ensure prompt notification of ITSD when there is a change in a City employee's role or employment status.
- ITSD does not have a formal program for computer security awareness.
- ITSD has not updated its business continuity/disaster recovery plan (BC/DR) since 2006, which consequently does not reflect current personnel, computing configurations, facilities, etc.

We recommend that ITSD management:

- Complete, document, and implement its plan for the IT Security Program.
- Work with City management to obtain approval to fill vacant IT security positions including the Chief Information Security Officer (CISO) position.
- Work with Human Resources (HR) to develop a process that will ensure ITSD is promptly notified of employee status changes.
- Implement an ongoing security awareness program that includes security training for all IT users.
- Update the BC/DR plan to reflect current conditions and staff.

Management's verbatim response is included at **Appendix E** on page 12.

Table of Contents

Executive Summary	i
Background	1
Audit Scope and Methodology	1
Internal Controls	2
Audit Results and Recommendations	3
A – Plan for IT Security	3
B - Security Roles and Responsibilities	3
C - Risk Assessment Policy and Procedures	4
D - Employee Transfer/Termination Procedures	4
E - Security Awareness Program	5
F - Business Continuity/ Disaster Recovery Policy and Procedures	6
G - Procedures for Security Incidents	6
Appendix A – ITSD Administrative Directives	8
Appendix B – COBIT Maturity Model	9
Appendix C – Information Technology Audit Schedule	10
Appendix D – Staff Acknowledgement	11
Appendix E – Management Responses	12

Background

Information Technology (IT) systems play a vital role in acquiring, processing, storing and distributing key financial, operational, and human resource related data at the City of San Antonio. The Information Technology Services Department (ITSD) provides IT services, 24 hours a day, 7 days a week to all City departments, delegate agencies, and various local, state, and federal government entities through information and technology sharing agreements. ITSD supports over 12,000 employees with computing and/or communication services.¹ ITSD has 237 budgeted full-time positions for fiscal year 2010 (a decrease of 3 positions from 2009 and 7 from 2008). Of the 237 budgeted positions, 36 are currently vacant.

The City's Chief Information Officer (CIO) hired an IT Security Supervisor, a new position, in October 2008. One of the Security Supervisor's responsibilities is to maintain reliable, secure, confidential, and continuous enterprise operations through policies, procedures, monitoring, risk assessment/planning/mitigation, recovery planning, and periodic testing. Fulfilling these responsibilities is the keystone to developing an effective security program. Six IT security-related AD's were in place prior to hiring the Security Supervisor. Since hiring the Security Supervisor, 6 more AD's/policies were approved and at least 11 more have been drafted (see **Appendix A** on page 8 for a list of ITSD Administrative Directives).

Filling the Security Supervisor position substantially improved the City's IT security posture. Recent accomplishments include implementing administrative directives (AD) pertaining to IT security, drafting a plan for the IT Security Program (ITSP), and establishing an IT security function with approved staff.

ITSD's recently drafted ITSP is expected to address all major systems and facilities and outline the duties of those who are responsible for overseeing security and those who own, use, or rely on the City's IT resources.

Audit Scope and Methodology

The scope of this audit included inquiries of City ITSD employees and review of documented policies and procedures provided by ITSD management. We also reviewed relevant documentation, such as risk assessments, security awareness training procedures, remediation of information security weaknesses, and security over activities performed by external third parties. We reviewed administrative directives, the ITSP draft, and the goals of ITSD pertaining to IT

¹ Office of Management and Budget, *Adopted Annual Budget Fiscal Year 2009*.

security. Additionally, we reviewed processes for assessing, monitoring, and responding to IT security threats.

We conducted this audit from July 2009 to December 2009 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate information to provide a reasonable basis for the results based on the audit objectives. We believe that the information obtained provides a reasonable basis for our audit results and conclusions based on our audit objectives. Our audit included tests of management controls that we considered necessary under the circumstances.

We obtained sufficient criteria and best practices for IT related processes and procedures. We used the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM). FISCAM presents a methodology for performing information system control audits in accordance with government auditing standards. Additionally, we relied on the IT Governance Institute's Control Objectives for Information and related Technology (COBIT version 4.1) for evaluating the maturity of IT internal controls.

FISCAM and COBIT are harmonized with other IT security standards including:

- NIST - National Institute for Standards and Technology
- ITIL - Information Technology Infrastructure Library
- FIPS - Federal Information Processing Standards

Internal Controls

Based on the Control Objectives for Information and related Technology (COBIT) maturity model for ensuring systems security², we concluded that overall, the maturity of ITSD's Information Security Program was "*Repeatable (2)*" but progressing towards "*Defined (3)*". This is because security awareness exists as evidenced by a number of recently issued IT security related administrative directives (AD's), but security plans and policies are not complete nor risk driven.

Maturity modeling is a method of evaluating internal controls in their current state against a maturity scale of non-existent (0) to optimized (5). The ultimate or target maturity level should be higher (e.g. 3, 4, or 5) rather than lower and should be influenced by ITSD and COSA business objectives, dependence on IT, technology sophistication, and most importantly, the value of the City's information. Our evaluation of controls for the observations in this audit and additional explanation of the different levels of the COBIT maturity model are included in **Appendix B** on page 9.

² IT Governance Institute – COBIT 4.1 DS5 – Deliver and Support – Ensure Systems Security, page 120.

Audit Results and Recommendations

A – Plan for IT Security

Although drafted, ITSD has not completed its plan for the IT Security Program (ITSP).

FISCAM Security Management section 1.1 (SM-1.1 on page 155) recommends that a plan for the security management program be developed, documented, and implemented to provide security for IT assets. Such a program is the foundation of an organization's IT internal control structure.

Without the ITSP, controls may be inadequate and responsibilities may be unclear, misunderstood, or improperly implemented. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

Recommendation: ITSD management should complete, document, and implement its plan for the IT Security Program. The plan should be in alignment with AD 7.8B Information Security Program.

B - Security Roles and Responsibilities

Although IT operations personnel perform certain security functions, ITSD currently has only one full-time dedicated IT security person.

In response to an IT Job Family Survey completed in the summer of 2008, ITSD management created the *IT Security Job Family*, which includes approved staffing for a Chief Information Security Officer (CISO), IT Security Supervisor, IT Security Lead, and an IT Security Analyst. However, only the IT Security Supervisor position is filled.

FISCAM Security Management section 1.2 (SM-1.2 on page 157) recommends that a security management structure (i.e. sufficiently staffed security function) be established to implement and enforce the information security program.

ITSD management indicated that due to a Citywide-hiring freeze, they could not fill the new security positions. A lack of sufficient security staff may result in significant risks to the City including inadequate management of IT security, poorly designed security controls, loss of IT assets, inappropriate access to and/or modification of critical data, disclosure of sensitive or personal data, unnecessary computer downtime, poor security awareness training, etc.

Recommendation: ITSD should determine the appropriate number of positions required to fill its IT security needs and work with City management to obtain approval to fill vacant positions including the CISO position.

C - Risk Assessment Policy and Procedures

Although, ITSD assesses risk and implements controls on an ad hoc basis, no policies or procedures exist for performing a structured IT risk assessment.

Risk assessments help make certain that threats and vulnerabilities are identified and considered, that the greatest risks are addressed, and that appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

FISCAM Security Management section 2 (SM-2 on page 166) recommends documenting risk assessment policies and procedures based on security categorizations of IT systems. Using a high, medium, low scale, this approach categorizes security relating to data confidentiality, integrity, and availability. A comprehensive risk assessment should be the starting point for developing or modifying an entity's security policies and security plans.

Lack of a risk management process may result in a gap between implemented controls (e.g. policies and procedures) and actual risks (i.e. threats) to IT assets. In other words, the City may be vulnerable to security threats for which it has no implemented controls due to not having performed a comprehensive risk assessment.

Recommendation: ITSD management should develop formal policies and procedures to perform IT risk assessments. In addition, ITSD should categorize IT systems to facilitate the risk assessment process.

D - Employee Transfer/Termination Procedures

There is no formal process in place to ensure that City departments promptly notify ITSD when there is a change in an employee's role or employment status.

FISCAM Security Management section 4.2 (SM-4.2 on page 178) recommends that security policies and procedures be in place to promptly notify security management of employee transfers or terminations in order to modify or revoke computer system and facility access.

Each City department is responsible for its own termination/transfer procedures. HR provides guidance (checklists) to departments on how to perform terminations and transfers, but no written policy requires departments to follow

the guidance. Related to this issue, the City Auditor observed the untimely removal of user access to the City's Hansen system in an audit report of the Planning and Development Services Department issued January 5, 2010.³

Untimely notification of changes in employee roles or employment status causes delays in required changes to IT system accesses and privileges. This delay could lead to unauthorized access to City computer systems, facilities, and other IT assets.

Recommendation: ITSD management should continue to work with HR to develop a process that ensures prompt notification to ITSD when an employee's status changes.

E - Security Awareness Program

ITSD does not have a formal program for computer security awareness.

FISCAM Security Management section 4 (SM-4 on page 176) recommends implementing an ongoing security awareness program that includes:

- first-time training for all new employees, contractors, and users
- periodic refresher training for all employees, contractors, and users
- distribution of security policies detailing rules and expected behaviors to all affected personnel

Currently, security awareness training is minimal and is being performed by HR. HR provides new COSA employees with an orientation packet that addresses 2 AD's related to security awareness; AD 7.4 Acceptable Use of Electronic Communications, and AD 7.5 Acceptable Use of Information Technology. New employees are required to read and sign an attached acknowledgement that they read the AD.

The lack of a security awareness program can result in employees or contractors inadvertently or intentionally compromising security. For example, employees could succumb to social engineering by revealing passwords or other sensitive information, or they could fall prey to security threats posed by spam (unsolicited commercial e-mail), spyware (software that monitors user activity without user knowledge or consent), or phishing (fraudulent messages to obtain personal or sensitive data).

Recommendation: ITSD management should develop and implement an ongoing security awareness program that includes security training for all IT users.

³ Office of the City Auditor – Audit of Building Permits Issuance and Collections Process – Project No. AU09-004, observation B.1 on page 6.

F - Business Continuity/ Disaster Recovery Policy and Procedures

ITSD has not updated its business continuity/disaster recovery plan (BC/DR) since 2006. This plan does not reflect current IT components including personnel, computing configurations, facilities, etc.

In 2006, ITSD completed and implemented a BC/DR plan. This plan created a BC/DR Response Team that is responsible for maintaining the plan and for ensuring that all personnel in their respective areas of operation within ITSD are trained on its use. Leading the Response Team is the BC/DR Manager who has the responsibility of directing the team and ensuring that the plan is maintained and up to date. However, the plan's named manager is no longer employed with ITSD and the plan does not address current IT asset (hardware and software) configurations, facilities, or ITSD staff and related responsibilities.

FISCAM Security Management section 1.1 (SM-1.1 on page 156) recommends that entity-wide information security programs include plans for the continuity of operations and information systems.

If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, financial losses, expensive recovery efforts, and inaccurate or incomplete information.

Recommendation: ITSD management should update the BC/DR Plan to reflect current conditions and staff. The BC/DR Plan should also include emergency training and related testing.

G - Procedures for Security Incidents

No formal policies or procedures exist for responding to IT security incidents such as hacking attempts. Additionally, there is no dedicated incident management team to monitor COSA's network for security incidents.

FISCAM Security Management section 1.1 (SM-1.1 on page 156) recommends implementing comprehensive procedures to detect, report, and respond to security incidents.

ITSD is continuing to enhance controls over critical systems by implementing advanced security appliances, software, and technology. Current policies, procedures, and standards are required to realize fully the benefits of this advanced security technology. Equally critical, a properly trained dedicated incident management team is necessary to respond to security breaches.

Without prompt and appropriate responses to security incidents, security breaches could occur, potentially causing significant damage to IT resources,

disclosure of confidential information, financial loss, and embarrassment to the City.

Recommendation: ITSD management should develop comprehensive procedures for detecting, reporting, and responding to security incidents. Additionally, ITSD should create and train a dedicated incident management team to monitor and respond to security incidents.

Appendix A – ITSD Administrative Directives

Administrative Directive	Formally Approved
AD 7-1 Automated Information Processing Policies and Procedures	8/1/1980
AD 7-2 Microcomputer Policies and Procedures	1/1/1990
AD 7-3 Data Security Policies and Procedures	10/5/1988
AD 7.4 Acceptable Use of Electronic Communication	11/29/2005
AD 7-5 Acceptable Use of Information Technology	11/15/2005
AD 7-6 Security and Passwords	11/29/2005
AD 7.5A Establishing IT Related Directives	9/29/2009
AD 7.8A Information Security Directive Summary	9/29/2009
AD 7.8B Information Security Program	9/29/2009
AD 7.8C Remote Access	9/29/2009
AD 7.8D Account Access Management	9/29/2009
AD 7.8E User Account Management	9/29/2009
AD 7.7A SAP Technology Standardization	In Process of being completed and formally approved.
AD 7.8F Electronic Signatures and Records	
AD 7.8G Encryption Standards Policy	
AD 7.8H Sensitive Information Management	
AD 7.8I Personally Identifiable Information Management	
AD 7.8J Payment Card Security Standards	
AD 7.8K Data Classification Policy	
AD 7.8L Disaster Recovery Standards Policy	
AD 7.8M Controls of Computer Virus and Malicious Code	
AD 7.8N Information Security for Contractors Vendors Third Parties	
AD 7.8P Information Technology Physical Security Guidelines	

Appendix B – COBIT Maturity Model

The COBIT maturity model for ensuring systems security⁴ is based on six levels of maturity which are paraphrased below:

0 Non-Existent: The organization does not recognize the need for IT security. Responsibilities and accountabilities are not assigned for ensuring security. Measures supporting the management of IT security are not implemented. There is no security reporting/response process for breaches.

1 Initial: The organization recognizes the need for IT Security, but security awareness depends on the individual. IT Security is addressed on a reactive basis and not measured.

2 Repeatable but Intuitive: Security awareness is fragmented and limited. IT Security information is generated, but is not analyzed. Security solutions tend to respond reactively to IT security incidents. Security policies are being developed.

3 Defined Process: Security awareness exists and is promoted by management. Security awareness briefings have been standardized and formalized. IT Security procedures are defined. An IT Security plan exists, driving risk analysis and security solutions.

4 Managed and Measurable: Responsibilities for IT security are clearly assigned, managed and enforced. IT security risk and impact analysis is consistently performed. Intrusion testing is a standard and formalized process leading to improvements.

5 Optimized: IT security requirements are clearly defined, optimized and included in a verified security plan. Periodic security assessments evaluate the effectiveness of implementation of the security plan. Incidents are promptly addressed with formalized procedures and automated tools.

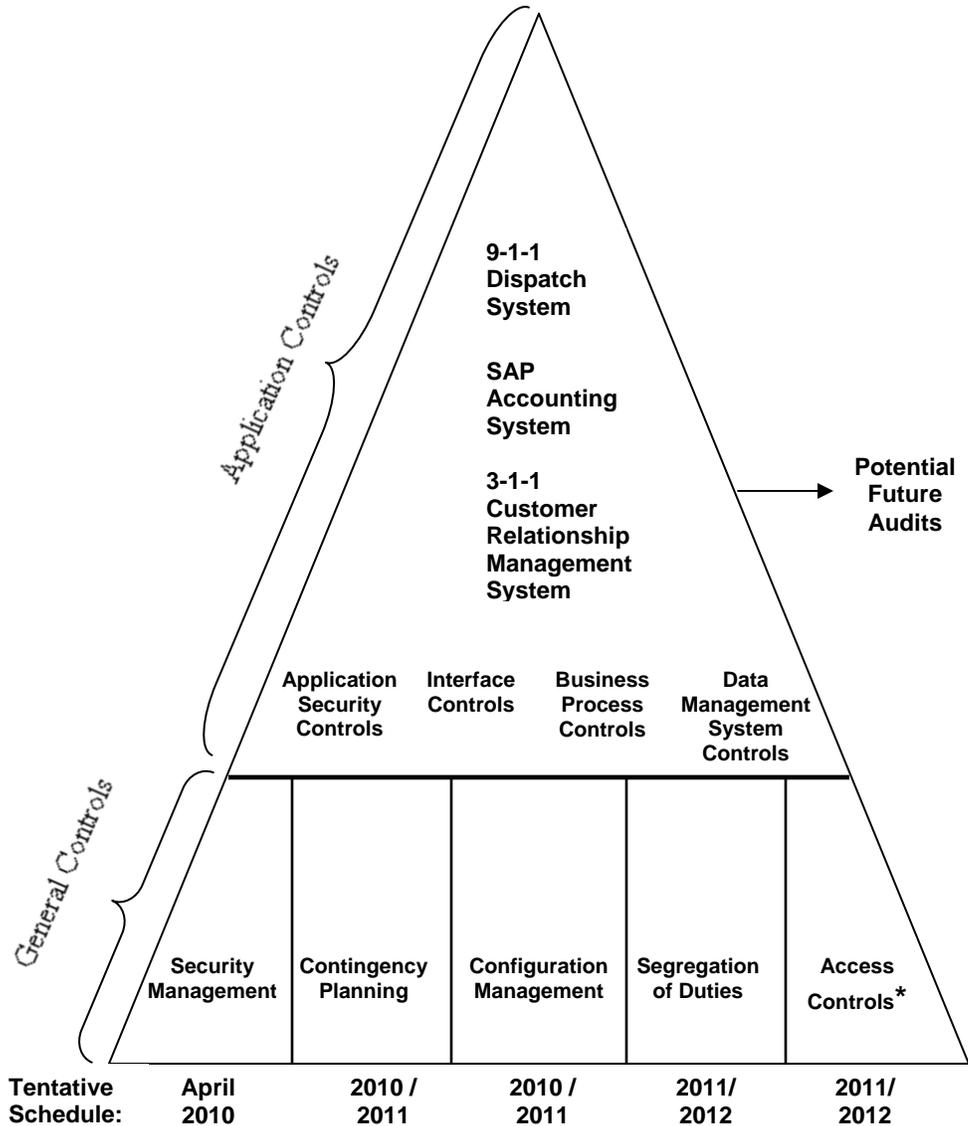
Based on the maturity levels above, we rated controls in ITSD’s information security program as shown below:

Observation	Information Security Program Test	0	1	2	3	4	5	Rating
A	Establish an information security program							2
B	Security responsibilities are clearly assigned							3
C	Perform a risk assessment							1
D	Establish organizational security							3
E	Develop a security awareness program							1
F	Establish an information security program							2
G	Remediate security weaknesses							3

⁴ IT Governance Institute – COBIT 4.1 DS5 – Deliver and Support – Ensure Systems Security, page 120.

Appendix C – IT Audit Schedule

Based on FISCAM Control Categories



* Access Controls include physical access security (e.g. data center access) and logical access security audits. Logical access security may include audits of system-level components such as the City's IT network (e.g. firewalls, web servers, routers), operating systems (server and workstation), and infrastructure application software (e.g. database management systems, identification and authentication systems, email/messaging systems, etc.).

Appendix D – Staff Acknowledgement

Barry Lipton, CPA, DABFA, Deputy City Auditor
Mark Bigler, CPA-Utah, CISA, CFE, Audit Manager
Gabe Trevino, CISA, Auditor in Charge
Alex Valadez, CISA, Auditor

Appendix E – Management Responses



CITY OF SAN ANTONIO

SAN ANTONIO TEXAS 78283-3966

April 27, 2010

Park E. Pearson, CPA
City Auditor
San Antonio, Texas

RE: Management's Corrective Action Plan for the Audit of the Information Security Program

ITSD has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

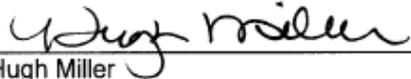
Recommendation					
#	Description	Audit Report Page	Accept, Partially Accept, Decline	Responsible Person's Name/Title	Completion Date
A	<p>Recommendation Title : IT Security Program Plan</p> <p>Recommendation: ITSD management should complete, document, and implement its plan for the IT Security Program. The plan should be in alignment with AD 7.8B Information Security Program.</p>	3	Accept	John Byers IT Security Supervisor	November 2010
<p>Action plan:</p> <ul style="list-style-type: none"> • An IT Security Plan is currently under development, and that plan aligns with AD 7.8B and principal areas of IT Security (Administration, Technical and Operational). • ITSD has a funded initiative currently underway to develop an IT Security Strategy, and when completed it will provide additional clarification to the IT Security Plan. 					
B.	<p>Recommendation Title: Security Roles and Responsibilities</p> <p>Recommendation: ITSD should determine the appropriate number of positions required to fill its IT security needs and work with City management to obtain approval to fill vacant positions including the CISO position.</p>	3	Accept	Bart Mulcahy ITSD AD	November 2010
<p>Action plan:</p> <ul style="list-style-type: none"> • ITSD has initially identified the need to staff the following IT Security positions: <ul style="list-style-type: none"> • One (1) Chief Information Security Officer (CISO) (funded, unfilled) • One (1) IT Security Supervisor (filled) • Two (2) IT Security Leads (both unfunded) • Two (2) IT Security Analysts (one advertised, one unfunded) • ITSD has initiated an internal study to determine the number of IT staff-hours currently dedicated to IT Security operations to determine if this staffing level is adequate. The findings of the study and recommendation will be published upon completion. • Positions will need to get approved and budgeted in the FY11 IT budget. Once approved we will work through the hiring process. 					

Recommendation					
#	Description	Audit Report Page	Accept, Partially Accept, Decline	Responsible Person's Name/Title	Completion Date
C.	<p>Recommendation Title: Risk Assessment Policy and Procedures</p> <p>Recommendation: ITSD management should develop formal policies and procedures to perform IT risk assessments. In addition, ITSD should categorize IT systems to facilitate the risk assessment process.</p>	4	Accept	CISO and John Byers	May 2010
<p>Action plan:</p> <ul style="list-style-type: none"> • Formal policies have been completed and others are in the final review process. These policies address Administrative, Technical and Operational processes to support IT security throughout the enterprise. • AD7.8D established that access to any information within COSA shall be based on factors including but not limited to compliance, best practices as established by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and relevant federal, state, and local statutes. • ITSD Policy 7-9000-x.002 v1.2 <i>Information Security Management Controls Policy</i> (currently in draft form and under review) requires that all City departments establish and maintain plans for conducting periodic risk assessments to ensure that appropriate, cost-justified safeguards are incorporated into existing or new information systems. • NIST Publication 800-30 <i>Risk Management Guide for Information Technology Systems</i> will provide the framework for risk management. • NIST Publication 800-53 <i>Recommended Security Controls for Federal Information Systems and Organizations</i> will provide the framework for risk assessment security controls. 					
D.	<p>Recommendation Title: Employee Transfer/Termination Procedures</p> <p>Recommendation: ITSD management should work with HR to develop a process that ensures prompt notification to ITSD when an employee's status changes.</p>	4	Accept		Complete
<p>Action plan:</p> <ul style="list-style-type: none"> • ITSD has had a formal process in place since 2008 to remove user access to SAP systems, mainframe applications, and the COSA network based on a change to their employment status in the City's HR system. Furthermore, AD7.8E (Para G) Account Termination states "COSA systems and/or applications shall include provisions for the timely termination of accounts. The process shall ensure that administrators who are tasked with terminating accounts are informed when users leave, transfer, or no longer need their access privileges". • Additional action by ITSD to ensure remediation will be to address the requirements for role-based security that shall include requirements for Provisioning, Change, and De-provisioning processes. The findings from the study shall be documented and shall establish the standards for all COSA for user account management. 					
E.	<p>Recommendation Title: Security Awareness Program</p> <p>Recommendation: ITSD management should develop and implement an ongoing security awareness program that includes security training for all IT users.</p>	5	Accept	John Byers IT Security Supervisor	December 2010

Recommendation					
#	Description	Audit Report Page	Accept, Partially Accept, Decline	Responsible Person's Name/Title	Completion Date
	<p>Action plan:</p> <ul style="list-style-type: none"> ITSD has worked with the City's HR Training organization to develop a comprehensive solution for delivering Security Awareness training and is finalizing the service requirements. ITSD is currently working with the UTSA Center for Infrastructure Assurance and Security (CIAS) to develop Security Awareness content and additional training material that is both COSA specific and generic in nature. This project includes a Learning Management System (LMS) for Security Awareness. 				
F.	<p>Recommendation Title: Business Continuity/ Disaster Recover Policy and Procedures</p> <p>Recommendation: ITSD management should update the BC/DR Plan to reflect current conditions and staff. The BC/DR Plan should also include emergency training and related testing.</p>	6	Accept	Ron Kliver IT Manager	December 2011
	<p>Action plan:</p> <ul style="list-style-type: none"> ITSD will be conduct a review of the existing BC/DR plans and will begin facilitating the development of a COSA-wide contingency program based on NIST Publication 800-34 <i>Contingency Planning for Information Technology Systems</i> to ensure compliance with ITSD Policy 7-9000-S.005 v1.4 <i>Information Asset Certification and Accreditation Policy (DRAFT)</i>. The contingency program will include an IT Contingency plan, an Incident Response plan and Disaster Recovery plans to support applications & systems requirements as defined by the needs of the individual information systems owners. ITSD shall provide the contingency plans for those information systems that are owned by ITSD. ITSD is in the process of identifying which systems and/or application are either Major System Applications (MSA) or General Service systems (GSS). Major System Applications are those that are critical to the organization's mission, including those that directly support Public Safety, Infrastructure, and Compliance. ITSD shall work to identify Critical Information Systems and Sensitive Information Systems collaboratively with the individual information system owners. ITSD will assign the Change Manager additional responsibilities to serve as the Continuity Manager also. 				
G.	<p>Recommendation Title: Procedures for Security Incidents</p> <p>Recommendation: ITSD management should develop comprehensive procedures for detecting, reporting, and responding to security incidents. Additionally, ITSD should create and train a dedicated incident management team to monitor and respond to security incidents.</p>	6	Accept	Diana Gonzalez Sr. IT Manager (ITSM)	May 2011
	<p>Action plan:</p> <ul style="list-style-type: none"> This will be addressed with the formulation of the Incident Response plan outlined in the response to Recommendation F - <i>Business Continuity/ Disaster Recovery Policy and Procedures</i> above. 				

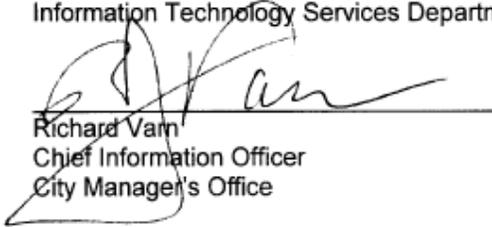
We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,



Hugh Miller
Director
Information Technology Services Department

April 27, 2010
Date



Richard Varn
Chief Information Officer
City Manager's Office

4/28/2010
Date