



CITY OF SAN ANTONIO

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

October 24, 2005

Phil Hardberger
Mayor

Kevin Wolf
Councilman, District 9

Art Hall
Councilman, District 8

Richard Perez
Councilman, District 4

Delicia Herrera
Councilwoman, District 6

Roger O. Flores
Councilman, District 1

Sheila D. McNeil
Councilwoman, District 2

Roland Gutierrez
Councilman, District 3

Patti Radle
Councilwoman, District 5

Elena Guajardo
Councilwoman District 7

Christopher "Chip" Haass
Councilman, District 10

J. Rolando Bono
City Manager

Ladies and Gentlemen:

RE: Confidential and Public final audit reports of "Aviation Network and Systems Security"

The audit for Aviation Network and Systems Security was performed during the summer 2005. This review was designed to assess the propriety of the internal control environment and risk management framework for the service processes associated with the Department's network and primary computing systems.

Two reports are being sent to you; one designated as "Confidential", the other "Public". Details of the "Confidential" report and this accompanying transmittal have been declared confidential due to the sensitivity of information in the report related to IT network and infrastructure security. As such, the "Confidential" report should not be discussed, copied or distributed without permission from the City Auditor, Department of Aviation, Information Technology Services Department (ITSD), and the City Attorney. The Public Information Act Section 552.139 addressing confidentiality of information relating to computer security issues is attached. The "Public" report excludes sensitive information and will be made available to the general public via the City Clerk's Office and the City Library.

These reports recommend the organizational reporting structure for Aviation IT should be changed such that it reports to the City's Information Technology Services Department (ITSD). The City's Chief Information Officer, Chief Technology Officer, and Aviation Department concur with the centralization of the IT staff. This should occur when the City's ITSD adopts specific IT practices and standards city-wide. ITSD indicated that staff alignment should be deferred until they have processes, policies and standards under more control.

These reports also recommend that security plans be developed and formalized for the Aviation network (wired and wireless) infrastructure and connected systems. The security plans should include provisions for the implementation of vulnerability testing procedures and secure wireless connectivity standards. These concerns are supported by the following issues identified during the audit:

- Firewall, intrusion detection, and incident handling control processes were not completed.
- Routine and periodic network vulnerability/penetration testing was not being performed.
- Strong wireless network standards had not been established.
- Formal continuity plans had not been developed.
- Service-level agreements do not exist.
- Environmental (fire) safeguards were not sufficient in Aviation computer rooms.

The Department has indicated that it plans to implement the recommendations related to IT security immediately, followed by the system reliability issues, and then work on improving service performance standards.

Finally, these reports included two repeat issues from a prior Aviation Department audit issued in January 2004:

- The Automated Parking System (APS) has been maintained and security access has been controlled by the Parking Manager which is not an appropriate segregation of duties.
- No surveillance devices had been installed in the Economy Parking Lot cashier booths.

Aviation Management indicated that it has implemented logical and physical security over the APS. However, the Department responded that the purchase of surveillance equipment would be dependent on approval of grant funding. The City Internal Audit Department points out that that this issue was a priority in the prior audit. Cashier booth surveillance equipment was also highlighted by the City-wide Cash Handling Initiative that began in December 2003 and is still on-going. The Aviation Parking operation, as an Enterprise Fund, generates substantial revenue to pay the relatively low cost to implement this recommendation. Therefore, this control should not be contingent upon approval of grant funding.

The audit team appreciated the cooperation and assistance extended by Aviation Department Systems staff and ITSD in performing this audit. The City Internal Audit Department is available to discuss the details of these reports with you at your individual convenience.

Sincerely,



Patricia M. Major CPA, CIA, CTP, CGFM
City Internal Auditor

Attachment

cc: Roland A. Lozano, Assistant to the City Manager and Interim Aviation Director
Michael Armstrong, CIO and Assistant City Manager
Erik Walsh, Assistant to the City Manager
Dom Smith, Assistant Aviation Director
Hugh Miller, CTO and Director, ITSD
Michael Bernard, City Attorney

- PUBLIC REPORT -



**CITY OF SAN ANTONIO
INTERNAL AUDIT DEPARTMENT**

Audit of Aviation Network and Systems Security



Project No. AU05-016

Release Date: October 24, 2005

Patricia Major CPA, CIA, CTP, CGFM
Mark Bigler CPA, CFE, CISA
Mark Swann CPA, CIA, CISA
Cynthia Munoz

EXECUTIVE SUMMARY

Overview

An audit of Aviation's network and system security has been completed. The objective of the audit was to review the adequacy of the internal control environment and risk management process related to network and systems security. Fieldwork for this audit was conducted primarily from May 2005 through June 2005. The audit was limited to a review of the Aviation Department's information technology (Aviation IT) "delivery and support" processes for ensuring network and systems security.

This audit was designed to provide reasonable, but not absolute, assurance that Aviation IT is effectively managing information and related technology, following best practices, and ensuring that internal controls are established and effective. This audit included a study of internal controls considered relevant mainly by the IT Governance Institute in assessing risks and the control environment. The audit was based on discussions, review of select documentation, and site visits. However, the procedures performed may not necessarily have revealed all internal control weaknesses.

The audit report includes background information to assist readers in understanding Aviation's organizational, staffing, technological, and operating environment.

Results In Brief

Aviation IT consists of three individuals who share responsibility with various contractors for all the technology needs of the Aviation Department, its tenants and customers. Currently, Aviation IT provides varying levels of support for the Department network and systems including finance, parking, flight information, operations, engineering, human resources, noise monitoring, and airport security. Aviation IT is currently involved with upgrading its network infrastructure and associated hardware, software, processes, procedures, and controls to support these various systems.

This audit identified certain security and control risks that should be addressed. The organizational reporting structure for Aviation IT should be changed such that it reports to the City's IT Services Department. Security plans should be developed and formalized for the Aviation network infrastructure. These security plans should also include provisions for the implementation of security testing standards.

Aviation IT resource availability should be enhanced by implementing continuity plans, formalizing backup procedures, and installing failover mechanisms. Also, incident management procedures should be developed and firewall logging activated.

Service level agreements should be developed with Aviation system users to avoid misunderstandings and to set expectations for appropriate levels of service. Finally, environmental safeguards for fire prevention and suppression in computer rooms need to be implemented.

Prior Audit Follow-up

The Internal Audit Department performed certain audit procedures which resulted in an audit report being issued in January 2004 titled '*Audit of Airport Parking Operations, Landing and Fuel Flowage Fees*'. Follow-up procedures were performed during fieldwork for this audit to determine if Aviation Management had implemented actions it promised in its responses to that audit. Based on follow-up work, Aviation Management should ensure that Parking personnel are precluded from performing security administrator functions within the Facility Management System (FMS) and that Aviation IT is assigned responsibility for all FMS operational aspects. Additionally, surveillance devices need to be installed in all cashier booths in the Economy Parking Lot and recording devices procured and installed to record cashier activity.

Background

San Antonio's Aviation facilities include the International Airport and the Stinson Municipal Airport. General and commercial aviation services are provided through an enterprise fund. The Aviation Department is directed by an acting Aviation Director who is an Assistant to the City Manager. Departmental responsibilities include airport operations, financial and property administration, economic development, vehicle and facility maintenance, airport security, fire protection, and public relations.

The San Antonio Airport is expected to facilitate about seven million passengers during 2005, and a daily average of about 250 international and domestic arrivals and departures. A 1995 Economic Impact Study performed by Ricondo and Associates in conjunction with the Airport Master Plan process showed that tenant activity at the Airport accounts for more than 11,000 jobs, over \$300 million in annual payroll, and over \$1 billion in additional economic sales and expenditures. Total funding from all sources for the Aviation Department for fiscal year 2005 was estimated to be \$263.2 million. This includes \$166.8 million earmarked for capital projects. Staffing expenses for over 400 full-time positions are also included in this estimate.

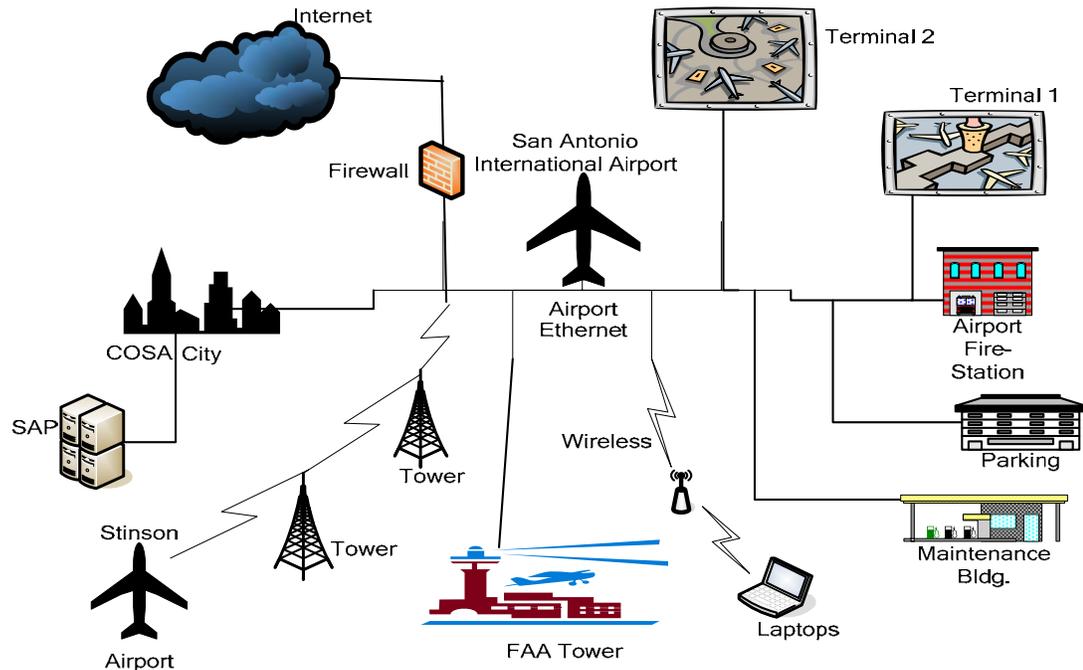
In alignment with the Airport Master Plan and Terminal Renovations Program which was approved by the Federal Aviation Administration (FAA) in 1998, Aviation Management adopted a number of initiatives to expand and upgrade general facilities at the City's Airports. These improvements include adding new terminals, extending runways, building new parking facilities, developing surrounding roadway systems, modernizing existing facilities, and upgrading the airport infrastructure among others.

Aviation IT Function

Aviation IT consists of three individuals who share responsibility with various contractors for all the technology needs of the Aviation Department, its tenants and customers. Aviation IT, to varying degrees, supports many vital systems including Airport Police Security (Fingerprint/Badge/"No-Fly" Data), Accounts Receivable, Mutual Usage Flight Information Display System (MUFIDS), Facility Management System (FMS) for airport parking, Automated Vehicle Identification System (AVIS), Noise Monitoring System (NOMS), Airfield Lighting Control, Engineering Computer Aided Design (CAD) System, Airport Operations Databank, Security Access Control (MATRIX), and others. Aviation IT also supports the network connecting all of these systems including links to the City of San Antonio (COSA) Systems (for using the SAP ERM System for example), the Internet, and the Stinson Municipal Airport (see **Exhibit 1** following).

Aviation IT plays an important role in providing network and system support to facilitate heightened security measures required by the United States Department of Homeland Security as a result of the 9/11 terrorist attacks. Homeland security measures are vital in protecting the millions of passengers who pass through the San Antonio International Airport every year in addition to the thousands of people who work at the airport and a half-billion dollars in airport assets.

Aviation Management's plans to upgrade the airport infrastructure included making improvements to certain components of the aging network infrastructure. These plans were documented in the *COSA IT Plan for FY 2001 – FY 2003*. Actual work on the Aviation IT network infrastructure did not begin until late 2004. It is not expected to be completed until later this summer, although many network components have been installed and are currently in use. The network infrastructure improvement includes upgrading network wiring and associated components, and installing a wireless network to support operations, airport security, and potentially airport passengers.

Exhibit 1 - Aviation Network**Aviation Network Environment**

The new network infrastructure being installed consists of the following components acquired from a sole vendor:

- **Switches** (simple network devices that select a path or circuit for sending data packets toward their destinations)
- **Routers** (more sophisticated than switches, routers are network devices that forward data packets toward their destinations using intelligence and routing tables)
- **Firewall** (a collection of specialized hardware, software, and network mechanisms designed to secure a computer or network from unauthorized access)
- **Wireless Access Points** (a communication device that allows the user of a wireless device such as a laptop or hand-held computer to connect to a wired network)
- **Intrusion Detection System (IDS)** (hardware and/or software used to detect unauthorized access to a computer system or network)

These network components facilitate access to various Aviation and COSA resources. The new Aviation network also includes wireless connectivity more generically known as "WiFi" or wireless fidelity. WiFi is a means of connecting to networks (e.g. Internet, COSA network, and the Aviation network) without the need of a physical cable. Installation of the wireless network had not been completed as of the end of fieldwork for this audit.

Security functions and responsibilities are shared between COSA IT and Aviation IT. Aviation users are authenticated at login time to the COSA network via the Microsoft active directory (AD) function which is maintained by the City's Information Technology Services Department (ITSD). After successful authentication, access to specific Aviation IT resources is governed by security and availability measures implemented solely by Aviation personnel for Aviation Systems (e.g. servers, databases, firewalls, et cetera).

Objectives

The objectives of this audit were to determine the adequacy and propriety of the internal control environment and risk management process related to the Aviation IT infrastructure including network and systems security. Ensuring the delivery of IT services requires a reliable and maintainable network infrastructure. This infrastructure should be designed for appropriate levels of availability based on service and security levels agreed upon by management. Furthermore, network and system availability is largely dependent on controls which should be designed to safeguard information (and related technology assets) against the effects of unauthorized use, disclosure, modification, or loss.

Scope

The scope of this audit included reviewing certain Aviation IT “delivery and support” processes for ensuring network and systems security including:

- Managing Security Measures
- Identification, Authentication and Access (for Remote Access Methods only)
- Network Security Surveillance and Violation Activity Reports
- Incident Handling
- Periodic Reaccreditation of Security
- Trusted Paths (i.e. a secure network)
- Firewall Architectures and Connections with Public Networks
- Malicious Software (a.k.a. malware) Prevention, Detection, and Correction
- Continuity Planning, Back-up Procedures, and Fault Tolerance Mechanisms
- Managing Facilities (Physical and Environmental Security)

All work was performed either at the office of the City Internal Audit Department or the San Antonio International Airport (Aviation Department). During this audit, no fieldwork occurred at the Stinson Airfield which has minimal IT resources, or the COSA ITSD.

Criteria

To measure performance, audit staff generally used criteria based on Control Objectives for Information and related Technology (CobiT), the Information Technology Infrastructure Library (ITIL), and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control – Integrated Framework.

The IT Governance Institute (www.itgi.org) developed CobiT as an open standard using non-technical language to help focus information technology in support of overall business goals. CobiT was selected as criteria for measurement because it is aimed at addressing business objectives and is easy to understand. CobiT continues to gain acceptance internationally and is evolving due to support from the IT Governance Institute.

ITIL (www.ogc.gov.uk) is an integrated set of best-practice recommendations drawn from public and private sectors internationally with common definitions and terminology covering IT service management areas such as incident, problem, change, capacity, availability, continuity, and service level agreement management.

The COSO Internal Control – Integrated Framework has been widely adopted as a best practice for documenting business process risks and internal controls for all publicly traded stock companies. This is mainly attributed to the federally mandated Sarbanes-Oxley Act of 2002 (SOX). This legislation was passed in response to corporate scandals such as Enron, WorldCom, Tyco and Global Crossing.

In addition to CobiT, ITIL, and COSO Internal Control – Integrated Framework, there are other industry based or technology specific practices that could be used to measure an organization’s control performance. The Center for Internet Security (CIS) and the SANS (SysAdmin, Audit, Network, Security) Institute both provide guidance on baselines to be used for enhancing control at a more detailed level. The Capability Maturity Model for Software (SW-CMM) could be used to judge the maturity of the software process and for identifying key practices that are required to advance the maturity of these processes.

It is important to note in reviewing the results of this audit that neither Aviation IT nor COSA ITSD has historically used these or any other standards to measure control performance related to IT service processes.

Methodology

The review was performed in compliance with generally accepted government auditing standards (GAGAS) issued by the U.S. Government Accountability Office (GAO) and other criteria to conform with the Institute of Internal Auditors’ “International Standards for the Professional Practice of Internal Auditing.”

Government Auditing Standards require a peer review of auditing practices at least once every three years by reviewers independent of the audit organization. The City Internal Audit Department (CIAD) had its last external peer review in July 2001. CIAD is scheduled for the next peer review in the summer of 2005.

In order to perform the work required, the audit staff used the following techniques:

- Conducted analyses to identify key internal controls encompassed within the Aviation network
- Made inquiries to Aviation IT staff and external subject matter experts
- Toured Aviation IT facilities
- Reviewed documentation provided by Aviation IT personnel
- Observed hardware components and their surrounding environments
- Researched IT technologies

Conclusion

After the completion of audit procedures, a conclusion was drawn on the completeness and viability of internal controls for ensuring Aviation network and systems security. The conclusion was formed through performing generally accepted audit procedures and was based on a Risk Management Capability Matrix. The risk matrix provides information on characteristics of development stages for strategy capabilities, process capabilities, people capabilities, technology capabilities, and information capabilities. For this project, the assessment was based specifically on process capabilities. A more detailed description of the process capability stages has been included as **Exhibit 2**.

While some Aviation IT processes exhibit higher levels of capability maturity, it was determined that the process capability maturity for ensuring Aviation network and systems security for the issues noted in this report are at the ‘Ad Hoc’ stage. This was based mainly on the observation that formal policies and procedures for many IT functions have not been developed. Aviation Management’s goal should be to strengthen IT service and security processes to the point where they are “Managed”. At the “Managed” stage, procedures and controls are well documented and kept current. Both preventive and detective controls are employed throughout the process. Many metrics are used, with a blend of automated and manual monitoring of performance.

Exhibit 2 – Process Capability Maturity Stages

<u>Stage</u>	<u>Procedures</u>	<u>Controls and Process Improvements</u>	<u>Metrics*</u>
Ad Hoc	<ul style="list-style-type: none"> No formal <i>procedures</i> exist. 	<ul style="list-style-type: none"> <i>Controls</i> are either non-existent, or are primarily reactionary after a “surprise” within the company. 	<ul style="list-style-type: none"> There are no <i>metrics</i> or monitoring of performance.
Repeatable	<ul style="list-style-type: none"> Some standard <i>procedures</i> exist. 	<ul style="list-style-type: none"> Detective <i>controls</i> are relied upon throughout the company. 	<ul style="list-style-type: none"> Few performance <i>metrics</i> exist, thus there is infrequent monitoring of performance.
Defined	<ul style="list-style-type: none"> <i>Procedures</i> are well documented, but are not regularly updated to reflect changing business needs. 	<ul style="list-style-type: none"> Both preventive and detective <i>controls</i> are employed throughout the company. 	<ul style="list-style-type: none"> Some <i>metrics</i> are used, but monitoring of performance is primarily manual.
Managed	<ul style="list-style-type: none"> <i>Procedures</i> and <i>controls</i> are well documented and kept current. 	<ul style="list-style-type: none"> Best practices and benchmarking are used to <i>improve</i> process in certain areas of the company. 	<ul style="list-style-type: none"> Many <i>metrics</i> are used, with a blend of automated and manual monitoring of performance.
Optimized	<ul style="list-style-type: none"> <i>Processes</i> and <i>controls</i> are continuously reviewed and <i>improved</i>. 	<ul style="list-style-type: none"> Extensive use of best practices and benchmarking throughout the company helps to continuously <i>improve</i> processes. 	<ul style="list-style-type: none"> Comprehensive, defined performance <i>metrics</i> exist, with extensive automated monitoring of performance employed.

*Metrics provide a means for measuring how well a control or process is performing.

*Source: 2004 Auditor’s Risk Management Guide, CCH Incorporated, 2004. Paul J. Sobel, CPA, CIA