



CITY OF SAN ANTONIO

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

June 13, 2012

Julián Castro
Mayor

Diego M. Bernal
Councilman, District 1

Ivy R. Taylor
Councilwoman, District 2

Leticia Ozuna
Councilwoman, District 3

Rey Saldaña
Councilman, District 4

David Medina, Jr.
Councilman, District 5

Ray Lopez
Councilman, District 6

Cris Medina
Councilman, District 7

W. Reed Williams
Councilman, District 8

Elisa Chan
Councilwoman, District 9

Carlton Soules
Councilman, District 10

SUBJECT: Audit Report of Information Technology Services Department - Segregation of Duties

Mayor and Council Members:

We are pleased to send you the audit report of the Information Technology Services Department (ITSD) - Segregation of Duties. This audit began in December 2011 and concluded with an exit meeting with department management in May 2012. Management's verbatim response is included in *Appendix D* 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,

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
City of San Antonio

Distribution:

Sheryl L. Sculley, City Manager
Ben Gorzell, Chief Financial Officer
Hugh Miller, Chief Technology Officer, Director – ITSD
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
Edward Benavides, Chief of Staff, Office of the City Manager
Donald Crews, Audit Committee Member
Stephen S. Penley, Audit Committee Member

CITY OF SAN ANTONIO
OFFICE OF THE CITY AUDITOR



Audit of Information Technology Services Department

Segregation of Duties

Project No. AU11-011

June 13, 2012

Kevin W. Barthold, CPA, CIA, CISA
City Auditor

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted an Information Technology Services Department (ITSD) segregation of duties audit with a focus on public safety systems. This audit is the fourth in a series of audits we performed over the past few years to assist ITSD by evaluating information technology general controls that apply to all or a large segment of the City's computer applications (see Appendix B on page 5 for our original IT audit schedule).

The audit objective, conclusion, and recommendation follow:

Are incompatible IT duties appropriately segregated?

Yes, we determined that incompatible IT duties are appropriately segregated. However, policies and procedures addressing segregation of duties need to be documented with regards to public safety systems.

We recommend that the Chief Technology Officer strengthen internal controls by documenting policies (a.k.a. "ITSD Standards") and procedures that appropriately segregate IT duties.

Information Technology Services Department management's verbatim response is in Appendix D on page 7.

Table of Contents

Executive Summary	i
Background.....	1
Audit Scope and Methodology	1
Internal Controls.....	2
Audit Results and Recommendations	3
A. Policies and Procedures	3
Appendix A – COBIT Maturity Model	4
Appendix B – IT Audit Schedule	5
Appendix C – Staff Acknowledgement.....	6
Appendix D – Management Response	7

Background

The Information Technology Services Department (ITSD) provides information technology (IT) services, 24 hours a day, seven days a week to all City departments, selected delegate agencies, and various local, state, and federal governmental entities through information and technology sharing agreements.

ITSD is structured as a centralized IT shared services organization that provides governance and support for the City's technology needs, including mission-critical public safety systems.

ITSD's goals and objectives relating to public safety systems are: "To provide oversight and support of the 911 communications center, major deployments and/or modifications of public safety systems, and all public safety information technology staff; to coordinate and implement a citywide security plan for all City facilities; and complete, implement and monitor an IT Strategic Plan for City Public Safety agencies".¹

By design, ITSD's organizational structure endeavors to divide key duties across multiple IT job types and groups in order to preclude one person from controlling all stages of a critical process. For example, the responsibility for programming is separated from the responsibility for moving software into production, and one programmer is not allowed to independently write, test, and approve program changes. ITSD also employs the principle of least privileged access to reduce the risk of unintended violations of segregation of incompatible duties.

During our audit, the City implemented a shared IT service support model. Accordingly, IT services previously provided by individual department personnel are now provided by personnel who report directly to ITSD management. Ostensibly, this change will provide a uniform and centrally managed support structure that will support consistency, integrity, and accountability so that departments can focus on core service delivery.

Audit Scope and Methodology

We interviewed ITSD management to obtain an audit universe of mission critical public safety systems. We focused our audit scope to review ITSD's roles with the mission critical public safety systems.

¹ City of San Antonio, Texas, *Adopted Annual Operating and Capital Budget - Fiscal Year 2012*, (San Antonio, 2011), 499.

We interviewed ITSD management, shared services personnel, and public safety staff and conducted reviews of relevant documentation including organizational charts, job descriptions, and privileged user access lists.

We conducted this audit from January 2012 through March 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our audit results and conclusions based on our audit objectives. We believe that the evidence 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.

To establish test criteria, we used the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM). The GAO's 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 standards are harmonized with other IT standards including those issued by the National Institute for Standards and Technology (NIST) and the Information Technology Infrastructure Library (ITIL).

Internal Controls

Based on the COBIT maturity model for ensuring internal controls, we concluded that, overall, the maturity of ITSD's Segregation of Duties was at level 2 "Repeatable but Intuitive," but progressing towards level 3 "Defined."² Although ITSD is committed to ensuring internal controls for segregation of duties are in place, no policies and procedures addressing segregation of incompatible duties for public safety systems were documented.

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 objectives (e.g. to apply the principle of least privileged access), dependence on IT, technology sophistication, and 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 A on page 4.

² IT Governance Institute – COBIT 4.1, page 175.

Audit Results and Recommendations

A. Policies and Procedures

IT shared services personnel had not documented segregation of duties policies and procedures relating to public safety systems.

FISCAM SD 3.1.1 recommends segregation of duties policies and procedures be documented.

A lack of formalized policies and procedures can lead to inadequately segregated duties that could directly impact the integrity of the City's public safety systems via improper program changes, fraudulent transactions, or damage/destruction to system resources.

Recommendation

The Chief Technology Officer should strengthen internal controls by documenting policies (a.k.a. "ITSD Standards") and procedures that appropriately segregate IT duties. The policies and procedures should address prohibited activities and privileged access.

Appendix A – COBIT Maturity Model

We rated the maturity of ITSD’s controls for segregation of duties as follows:

Observation	Segregation of Duties	0	1	2	3	4	5	Rating
A	Policies and Procedures							2

The COBIT maturity model for ensuring internal control of segregation of duties is based on six levels of maturity, which are paraphrased below:

0 Non-existent: There is no recognition of the need for internal control. Control is not part of the organization’s culture or mission. There is a high risk of control deficiencies and incidents.

1 Initial/Ad Hoc: There is some recognition of the need for internal control. The approach to risk and control requirements is *ad hoc* and disorganized, without communication or monitoring. Deficiencies are not identified. Employees are not aware of their responsibilities.

2 Repeatable but Intuitive: Controls are in place but are not documented. Their operation is dependent on knowledge and motivation of individuals. Effectiveness is not adequately evaluated. Many control weakness exist and are not adequately addressed; the impact can be severe. Management actions to resolve control issues are not prioritized or consistent. Employees may not be aware of their responsibilities.

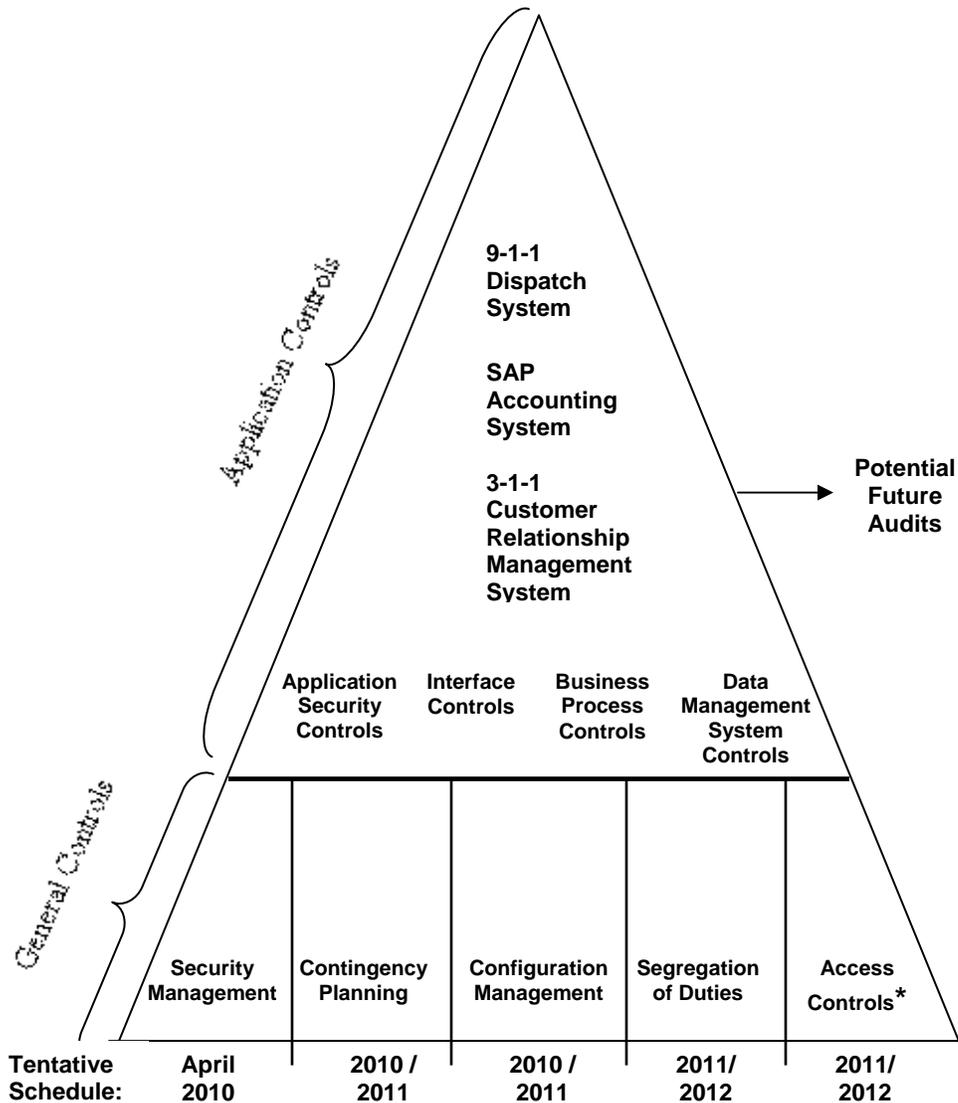
3 Defined: Controls are in place and are adequately documented. Operating effectiveness is evaluated on a periodic basis and there is an average number of issues. However, the evaluation process is not documented. Whilst management is able to deal predictably with most control issues, some control weaknesses persist and impacts could still be severe. Employees are aware of their responsibilities for control.

4 Managed and Measurable: There is an effective internal control and risk management environment. A formal, documented evaluation of controls occurs frequently. Many controls are automated and regularly reviewed. Management is likely to detect most control issues, but not all issues are routinely identified. There is consistent follow-up to address identified control weakness. A limited, tactical use of technology is applied to automate controls.

5 Optimized: An enterprise-wide risk and control program provides continuous and effective control and risk issues resolution. Internal control and risk management are integrated with enterprise practices, supported with automated real-time monitoring with full accountability for control monitoring, risk management and compliance enforcement. Control evaluation is continuous, based on self-assessments and gap and root cause analyses. Employees are proactively involved in control improvements.

Appendix B – IT Audit Schedule

Based on FISCAM Control Categories



*Access Controls include physical access security (e.g. data center access) and logical access security. 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 (e.g. server, workstation), and infrastructure application software (e.g. database management systems, identification and authentication systems, email/messaging systems, etc.).

Appendix C – Staff Acknowledgement

Mark Bigler, CPA-Utah, CISA, CFE, Audit Manager
Alex Valadez, CISA, CBRM, CBRA, Auditor in Charge
Matthew Howard, CISA, Auditor
Raymond Scott Miller, CFE, CIA, MBA, Auditor

Appendix D – Management Response



CITY OF SAN ANTONIO

SAN ANTONIO TEXAS 78283-3966

June 7, 2012

Kevin W. Barthold, CPA, CIA, CISA
City Auditor
San Antonio, Texas

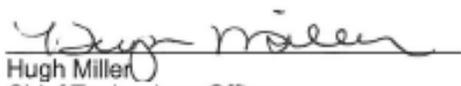
RE: Management's Corrective Action Plan for the IT Segregation of Duties Audit

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: Policies and Procedures</p> <p>Recommendation: The Chief Technology Officer should strengthen internal controls by documenting policies (a.k.a. "ITSD Standards") and procedures that appropriately segregate IT duties. The policies and procedures should address prohibited activities and privileged access.</p>	3	Accept	Patsy Boozer /CISO	November 2012
<p>Action plan:</p> <p>ITSD has in place the documents below that relate to proper account management and segregation of duties for software systems.</p> <ul style="list-style-type: none"> • AD7.8D and AD 7.8E established that ITSD, shall ensure the effective administration of their IT staff's access to information and IT resources in order to maintain necessary security levels and to the extent possible, implement role-based access appropriate to the sensitivity levels and responsibilities of the IT position. • ITSD Policy 7-9000-S.003v1.5 <i>Information Security Operational Controls Policy</i> requires that access to information assets include appropriate segregation of duties and use of the least privilege security principle. <p>To further enhance account management and proper segregation of duties, ITSD will develop the documents below:</p> <ul style="list-style-type: none"> • ITSD will develop an <i>Access Control Management Standard</i> to include management of information systems and resources in a manner that supports role based access, separation of duties and the principle of least privilege in compliance with AD7.8D and AD 7.8E and ITSD Policy 7-9000-S.003v1.5. • ITSD will develop an <i>ITSD Access Control Management Standard – Procedural Guidelines</i> that provide procedures to implementation best practices based on NIST 800-53A for separation of duties/access control for IT staff (i.e. DBA/sys admin segregation and access control). Procedures will include a process for updating accounts when privileged users change job functions, leave, no longer require access, etc as well as a quarterly review of the privileged accounts on critical systems. 					

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

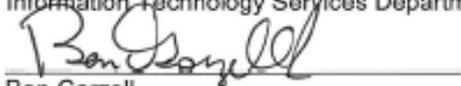
Sincerely,



Hugh Miller
Chief Technology Officer
Information Technology Services Department

06/07/2012

Date



Ben Gorzell
Chief Financial Officer
City Manager's Office

6/7/2012

Date