



CITY OF SAN ANTONIO

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

October 25, 2013

Julián Castro
Mayor

Rebecca J. Viagran
Councilwoman, District 3

Ray Lopez
Councilman, District 6

Carlton Soules
Councilman, District 10

Diego M. Bernal
Councilman, District 1

Rey Saldaña
Councilman, District 4

Cris Medina
Councilman, District 7

Ivy R. Taylor
Councilwoman, District 2

Shirley Gonzales
Councilwoman, District 5

Ron Nirenberg
Councilman, District 8

SUBJECT: Follow-up Audit of Information Technology Services Department - IT Contingency Planning

Mayor and Council Members:

We are pleased to send you the final report of the follow-up audit of the Information Technology Services Department – IT Contingency Planning. This audit began in July 2013 and concluded with an exit meeting with department management in August 2013. Management’s verbatim response is included in Appendix B of the report. The Information Technology Services Department’s management and staff should be commended for their 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,

A handwritten signature in black ink, appearing to read 'Kevin W. Barthold'.

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 and ITSD Department Director

Patsy Boozer, Chief Information Security Officer

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



Follow-up Audit of Information Technology Services Department

IT Contingency Planning

Project No. AU13-F05

October 25, 2013

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

Executive Summary

As part of our annual Audit Plan approved by City Council, we conducted a follow-up audit of the recommendations made in the Audit of Information Technology Services Department (ITSD) IT Contingency Planning dated March 9, 2012. The audit objectives, conclusions, and recommendations follow:

Has ITSD management implemented sufficient contingency action plans?

ITSD has effectively implemented action plans that address all but one of the five recommendations from the March 2012 report.

The prior audit recommended that the Chief Technology Officer:

- Work with the City Manager's Office to facilitate the development of a CoSA-wide contingency program.
- Develop the contingency program to include IT contingency, incident response, and disaster recovery plans to support applications and system requirements as defined by the needs of individual systems owners.
- Continue with the development of the Application Inventory System and coordinate with City departments to update its information on a timely basis to reflect the City's current IT environment.
- Continue to collaborate with individual information systems. The Chief Technology Officer should do this in conjunction with the recommendation for observation C above to develop the Application Inventory System.
- Assign continuity management responsibilities to an appropriate ITSD individual and expedite the filling of all related open IT positions.

The Chief Technology Officer (CTO) and the City Manager's Office (CMO) facilitated the creation of a CoSA-wide contingency program that includes an IS Contingency Plan (ISCP), Business Continuity Plan (BCP), and a Disaster Recovery Plan (DRP). In collaboration with City departments, the CTO also developed an Application Inventory System identifying critical/sensitive and non-critical information systems. Although ITSD has filled all IT positions within the IT security group, the Business Continuity Manager (BCM) position has not been established.

We recommend that the Chief Technology Officer establish the BCM role to oversee the CoSA-wide contingency program.

ITSD's Management's verbatim response is in Appendix B on page 5.

Table of Contents

Executive Summary	i
Background	1
Audit Scope and Methodology	1
Audit Results and Recommendations	2
A. CoSA-wide Contingency Plan.....	2
B. Contingency Program.....	2
C. Identification of Major System Applications	2
D. Identification of Critical/Sensitive Information Systems	3
E. Assignment of Continuity Manager Responsibilities	3
Appendix A – Staff Acknowledgement	4
Appendix B – Management Response	5

Background

In March of 2012, the Office of the City Auditor completed an audit of IT Contingency Planning. The objective of that audit was as follows:

Has ITSD management implemented sufficient contingency action plans?

The Office of the City Auditor concluded that ITSD had not implemented contingency planning actions. Specifically, ITSD had not started the development of a CoSA-wide contingency program or supporting contingency and disaster recovery (DR) plans. ITSD had not assigned continuity manager responsibilities or filled open security positions.

Audit Scope and Methodology

The audit scope was limited to the recommendations made in the original report and corresponding action plans implemented between March 2012 and April 2013.

The audit methodology consisted of reviewing current federal regulations relevant to contingency planning, CoSA-wide contingency planning policies and procedures, and supporting business continuity planning documentation. We also interviewed ITSD management to ensure the development of a CoSA-wide contingency program.

We conducted this follow-up performance audit 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 findings and conclusions based on our audit objectives.

We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results and Recommendations

A. CoSA-wide Contingency Plan

The Chief Technology Officer should work with the City Manager's Office to facilitate the development of a CoSA-wide contingency program.

Status: Implemented

The Chief Technology Officer (CTO) and the City Manager's Office (CMO) facilitated the creation of a CoSA-wide contingency program. The contingency program includes a Continuity of Operations Plan (COOP) for each of the business areas. During the creation of the COOPs, a Business Impact Analysis (BIA) and a Privacy Impact Assessment (PIA) was created in order to prioritize business processes based on criticality and recovery times.

B. Contingency Program

The Chief Technology Officer should develop the contingency program to include IT contingency, incident response, and disaster recovery plans to support applications and system requirements as defined by the needs of individual systems owners. In addition, the Chief Technology Officer should develop contingency plans for those information systems that are owned by ITSD.

Status: Implemented

The Chief Technology Officer has created a contingency program that includes an IS Contingency Plan (ISCP), Business Continuity Plan (BCP), and a Disaster Recovery Plan (DRP). These specific IT contingency plans contain a broad scope incorporating procedures and capabilities suited to sustaining mission critical business operations, alternate information system relocation sites, and information system recovery and/or restoration in the event of an emergency.

C. Identification of Major System Applications

The Chief Technology Officer should continue with the development of the Application Inventory System and coordinate with City departments to update its information on a timely basis to reflect the City's current IT environment.

Status: Implemented

The Chief Technology Officer has developed an Application Inventory System in coordination with City departments to reflect the City's current IT environment. Major

system applications and/or general service applications have been identified in addition to prioritizing mission essential applications, software type, manufacturer, platform type, locations, and availability requirements.

D. Identification of Critical/Sensitive Information Systems

The Chief Technology Officer should continue to collaborate with individual information system owners. The Chief Technology Officer should continue with the development of the critical/sensitive and non-critical information system inventory.

Status: Implemented

The Chief Technology Officer has created an information system inventory identifying critical/sensitive and non-critical information systems. In collaboration with City departments, the inventory identifies supporting resources such as hardware, software, and system documentation.

E. Assignment of Continuity Manager Responsibilities

The Chief Technology Officer should assign continuity management responsibilities to an appropriate ITSD individual and expedite the filling of all related open IT positions.

Status: Partially Implemented

Although ITSD has filled all IT positions within the IT security group, the Business Continuity Manager (BCM) position has not been established. The BCM role would oversee the CoSA-wide contingency program through actively monitoring and/or maintaining individual departmental contingency plans. In addition, the BCM would assist departments in departmental tests, training, and exercise plans. If the BCM role remains vacant, the CoSA-wide contingency program could become outdated and ineffective.

Recommendation:

We recommend that the Chief Technology Officer establish the BCM role to oversee the CoSA-wide contingency program.

Appendix A – Staff Acknowledgement

Mark Bigler, CPA-Utah, CISA, CFE, Audit Manager
Gabe Trevino, CISA, Auditor in Charge
Michael Hurlbut, Auditor

Appendix B – Management Response



CITY OF SAN ANTONIO
SAN ANTONIO TEXAS 78283-3966

September 6, 2013

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

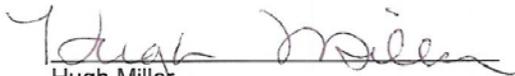
RE: Management's Corrective Action Plan for Follow-up Audit of the Information Technology Services Department IT Contingency Planning

Information Technology Services Department has reviewed the audit report and has developed the Corrective Action Plans below corresponding to report recommendations.

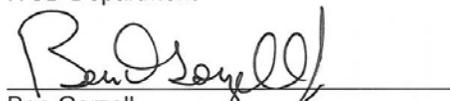
Recommendation					
#	Description	Audit Report Page	Accept, Decline	Responsible Person's Name/Title	Completion Date
1	Assignment of Continuity Manager Responsibilities Establish the BCM role to oversee the CoSA-wide contingency program.	3	Accept	Hugh Miller	Nov 2013
<p>Action plan: The Chief Technology Officer (CTO) will work with the Office of Emergency Management (OEM) Director to ensure the responsibilities of a BCM to work with City department BCP's to oversee the CoSA-wide contingency program are fulfilled through the collaboration of ITSD and OEM existing positions.</p>					

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

Sincerely,


Hugh Miller
Director
ITSD Department

10/16/2013
Date


Ben Gorzell
Chief Financial Officer

10/17/2013
Date