



CITY OF SAN ANTONIO

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

March 9, 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 – IT Contingency Planning

Mayor and Council Members:

We are pleased to send you the audit report of Information Technology Services Department – IT Contingency Planning. This audit began in September 2010 and concluded with an exit meeting with department management in November 2011. Management's verbatim response is included in Appendix E of the report. The Information Technology Services Department 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,

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

IT Contingency Planning

Project No. AU10-010

March 9, 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) contingency planning¹ audit. This audit is one of several audits we will perform over the next 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 9 for our tentative IT audit schedule).

The original audit objective was to determine if controls are in place to minimize the risk of unplanned interruptions to IT services and provide recovery of critical operations. Due to a significant overlap in planned tests for the original objective and tests previously performed for our ITSD Information Security Program audit report issued May 13, 2010, we modified our objective to the following:

Has ITSD management implemented sufficient contingency action plans?

No, ITSD has not implemented contingency planning actions as stated in its response to recommendations made in the Information Security Program audit mentioned above.

ITSD has begun the process of identifying and categorizing COSA systems and applications with respect to criticality and sensitivity in order to facilitate contingency planning and recovery efforts. However, we observed that:

- ITSD has not started the development of a COSA-wide contingency program or supporting contingency and disaster recovery (DR) plans.
- ITSD has not assigned continuity manager responsibilities or filled open security positions.

We recommended that the Chief Technology Officer:

- Work with the City Manager's Office to develop a contingency program.
- Develop the contingency program to include IT contingency, incident response, and disaster recovery plans to support applications and system requirements.
- Assign continuity management responsibilities to an appropriate ITSD individual and expedite the filling of all open related IT positions.

Management's verbatim response is in Appendix E on page 13.

¹ See Appendix C on page 11 for a description of contingency planning.

Table of Contents

Executive Summary	i
Background	1
Audit Scope and Methodology	2
Internal Controls	2
A. COSA-Wide Contingency Plan	4
B. Contingency Program	5
C. Identification of Major System Applications.....	6
D. Identification of Critical/Sensitive Information Systems.....	6
E. Assignment of Continuity Manager Responsibilities.....	7
Appendix A – COBIT Maturity Model	9
Appendix B – IT Audit Schedule.....	10
Appendix C – Contingency, Disaster Recovery, and Continuity Planning	11
Appendix D – Staff Acknowledgement	12
Appendix E – Management’s Responses	13

Background

The Information Technology Services Department (ITSD) provides information technology (IT) services 24 hours a day, 7 days a week to all City departments, 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 all technology functions and builds information systems around IT industry best practices that facilitate the goals and objectives of the City of San Antonio.²

ITSD's security service goals and objectives are to "Maintain reliable, secure, confidential, and continuous enterprise operations through policies, procedures, monitoring, risk assessment/planning/mitigation, recovery planning, and periodic testing. This will provide high availability of enterprise information technology resources through protection from and prevention of cyber incidents, as well as business continuity (BC) efforts."³

To facilitate continuous operations, ITSD utilizes a hot site, the Emergency Operations Center (EOC). The EOC hot site is an operational off-site processing facility equipped with hardware, software, and networking services required for full recovery in the event of a disaster or interruption of the City's Frio Street computing operations. ITSD has implemented significant security services controls to facilitate continuous operations. These controls minimize single points-of-failure and include the following at both data centers (Frio Street and EOC):

- Power redundancy controls (e.g. multiple diesel generators, uninterruptible power supplies (UPS), power distribution units (PDU))
- Multiple heating ventilation air conditioning (HVAC) units to control computer room temperatures and prevent overheating
- Data center configuration changes for better cooling and airflow
- Routine preventive maintenance on power redundancy and temperature controls to ensure functionality
- 24/7 power, data, and network monitoring services
- Server and data storage virtualization⁴

² City of San Antonio, Texas, *Balanced Adopted Annual Operating and Capital Budget - Fiscal Year 2011*, (San Antonio, 2010), 508.

³ *Balanced*, 509.

⁴ Virtualization uses failover and high availability mechanisms, which minimizes downtime. Failover and high availability enable the launching of a new instance of an application immediately if the first instance stops working for any reason.

Audit Scope and Methodology

We reviewed procedures for minimizing the risk of unplanned interruptions and plans to recover critical operations should interruptions occur. We interviewed ITSD and EOC staff and conducted reviews of relevant documentation including the 2006 draft contingency plan, service level agreements, contracts, system maintenance reports for environmental controls, and procedures pertaining to business continuity (see **Appendix C** which shows the relationship between contingency, disaster recovery, and continuity planning).

We conducted this audit from September 2010 to May 2011 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.

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). 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 continuous service, we concluded that overall, the maturity of ITSD's IT Contingency Plan was at level 2 "Repeatable but Intuitive," but progressing towards level 3 "Defined."⁵ Although ITSD is committed to continuous service availability, it has no documented contingency plan.

⁵ IT Governance Institute – COBIT 4.1 Deliver and Support – Ensure Continuous Service, page 116

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 provide continuous enterprise operations), 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 9.

Prior Action Plans and Audit Results

A. COSA-Wide Contingency Plan

ITSD management stated that it would conduct a review of the existing BC/DR plans and begin facilitating the development of a COSA-wide contingency program based on NIST Publication 800-34 Contingency Planning for Information Technology Systems to ensure compliance with ITSD Policy 7-9000-S.005 v1.4 Information Asset Certification and Accreditation Policy (DRAFT). ITSD management indicated that it would implement this corrective action plan by December 2011.

ITSD's current action plan status and response follows:

ITSD has assessed current versions of the BC/DR plans in order to determine the level of effort required to update and bring the various DR plans in compliance to the various standards.

ITSD contracted with AT&T to conduct a security gap-analysis for our Health Insurance Portability and Accountability (HIPAA) and Payment Card Industry (PCI) implementations. This gap-analysis in conjunction with ongoing efforts of ITSD provides a base for implementation of an enterprise-wide IT strategy for BC/DR planning. In addition, ITSD had a consultant conduct a security review with a focus on security controls and related maturity. The result of this review is the Security Strategic Plan⁶ which will provide the framework for future growth and continued development in this area.

In reviewing the requirements of NIST 800-34, ITSD cannot adequately develop all plans as required. An overarching contingency plan for the City should be developed to provide governance for business resumption. Without a City-wide effort, BC plans are developed in a silo without the necessary governance and instructions. ITSD can develop an IT Contingency Plan but the plan will lack certain elements, which are normally part of a business continuity plan (BCP).

Based on the action plan status above, ITSD is not on track to facilitate the development of a COSA-wide contingency program by December 2011.

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

⁶ The purpose of the Information Security Strategic Plan is to identify the security goals and objectives of the City and build a high level, risk-based plan to meet them.

B. Contingency Program

ITSD management stated that the contingency program will include an IT Contingency plan, an Incident Response plan and Disaster Recovery plans to support applications and 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 management indicated that it would implement this corrective action plan by December 2011.

ITSD's current action plan status and response follows:

ITSD has enhanced controls over critical systems by implementing advanced security appliances, software, and technology. Current policies, procedures, and standards have been developed for advanced security technology.

ITSD is currently developing an enhanced IT Security Awareness program. The program will address, in addition to security awareness, various other training as required for IT services.

ITSD works with the City's Emergency Operations Center⁷ (EOC) and State agencies in improving IT incident response and regularly participates in various local and statewide exercises, including the Cyber Security Exercise Phase III (May 2011). ITSD has members who are part of the FBI InfraGard⁸, which provides training and information on incident management and handling.

ITSD is working to complete an inventory of application systems as outlined in observation C below. This will provide an inventory of Enterprise (ITSD) and Department applications. The inventory will provide key information for the development of various plans.

ITSD is developing certain incident response capabilities and enhancing security. However, it is not progressing towards developing a contingency program supported by contingency and disaster recovery plans by December 2011.

Recommendation: 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

⁷ The Emergency Operations Center houses the communication, coordination, command and control elements of the response to catastrophic, all-hazard events in a state-of-the-art facility located in a secure location. The 36,000-square foot facility includes a dedicated policy room, command and operations room, a media briefing room, space for regional medical operations support, administrative and support space, technical infrastructure and redundant communications systems and electrical backup generator systems.

⁸ InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and the private sector. It is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States.

should develop contingency plans for those information systems that are owned by ITSD.

C. Identification of Major System Applications

ITSD management stated that it is in the process of identifying which systems and/or applications 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 management indicated that it would implement this corrective action plan by December 2011.

ITSD's current action plan status and response follows:

ITSD has developed the Application Inventory System to capture enterprise and department applications that include the necessary elements for MSA and GSS. The system also includes information identifying those systems, which support Public Safety.

The application inventory system includes elements that are part of BC/DR in determining the criticality of the application/system. The system provides for security classifications of systems classified as PUBLIC or CONFIDENTIAL and data types for HIPAA, PCI, personally identifiable information (PII), and PUBLIC SAFETY.

Auditors determined that ITSD has begun the process of identifying and categorizing COSA systems and applications. ITSD has completed populating the Application Inventory System with applications, and is in the process of categorizing those applications.

Recommendation: 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.

D. Identification of Critical/Sensitive Information Systems

ITSD management stated that it will work to identify critical and sensitive information systems collaboratively with the individual information system owners. ITSD management indicated that it would implement this corrective action plan by December 2011.

ITSD's current action plan status and response follows:

ITSD has catalogued over 1,000 applications to-date in the Application Inventory System. This system includes the identification of application and system criticality and the classification of related information and data. ITSD intends to continue to refine and develop the system as well as continue its efforts in application inventory management.

ITSD has undertaken a major effort to refine the information in the system and to update information that is missing.

ITSD continues to develop and refine the physical inventory of all hardware. This information will, when completed, be uploaded to the BMC Remedy system as part of an overall IT Management solution.

Auditors determined that ITSD has begun the process of identifying and categorizing critical and sensitive systems and applications as mentioned in observation C above.

Recommendation: The Chief Technology Officer should continue to collaborate with individual information system owners on a timely basis to identify critical and sensitive information systems. The Chief Technology Officer should do this in conjunction with the recommendation for observation C above to develop the Application Inventory System.

E. Assignment of Continuity Manager Responsibilities

ITSD management stated that it would assign the Change Manager additional responsibilities to serve as the Continuity Manager. ITSD management indicated that it would implement this corrective action plan by December 2011.

ITSD's current action plan status and response follows:

The position of Chief Information Security Officer (CISO) or Infrastructure Director will assume the duties and responsibilities of Continuity Manager. This position will coordinate the efforts of BC/DR and change management for ITSD. Currently there are three unfilled senior level positions. Additionally an IT Security Lead position has been approved however it is not funded and is needed by the organization to assist in these areas.

ITSD management has interviewed candidates for these ITSD security positions, and has made offers. However, candidate salary requirements have exceeded ITSD's salary range resulting in these positions remaining unfilled.

Based on the action plans above, ITSD has not assigned continuity manager responsibilities.

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

Appendix A – COBIT Maturity Model

We rated the maturity of ITSD’s controls for contingency planning as follows:

Observation	IT Contingency Planning	0	1	2	3	4	5	Rating
A	COSA-Wide Contingency Plan							2
B	Contingency Program							2
C	Identification of Major System Applications							2
D	Identification of Critical/Sensitive Systems							2
E	Assignment of Continuity Responsibilities							2

The COBIT maturity model for ensuring continuous service is based on six levels of maturity, which are paraphrased below:

0 Non-existent: Management does not consider service continuity a need. There is no understanding of the risks, vulnerabilities and threats to IT operations or the impact of loss of IT services.

1 Initial/Ad Hoc: Management considers service continuity a need but its focus is on infrastructure resources rather than IT services. Responsibilities are informal and authority to execute responsibilities is limited. IT response to major disruptions is reactive and unprepared.

2 Repeatable but Intuitive: Responsibility for ensuring continuous service is assigned. The approaches to ensuring continuous service are fragmented. There is no documented IT continuity plan, although there is commitment to continuous service availability. Continuous service practices are emerging, but success relies on individuals.

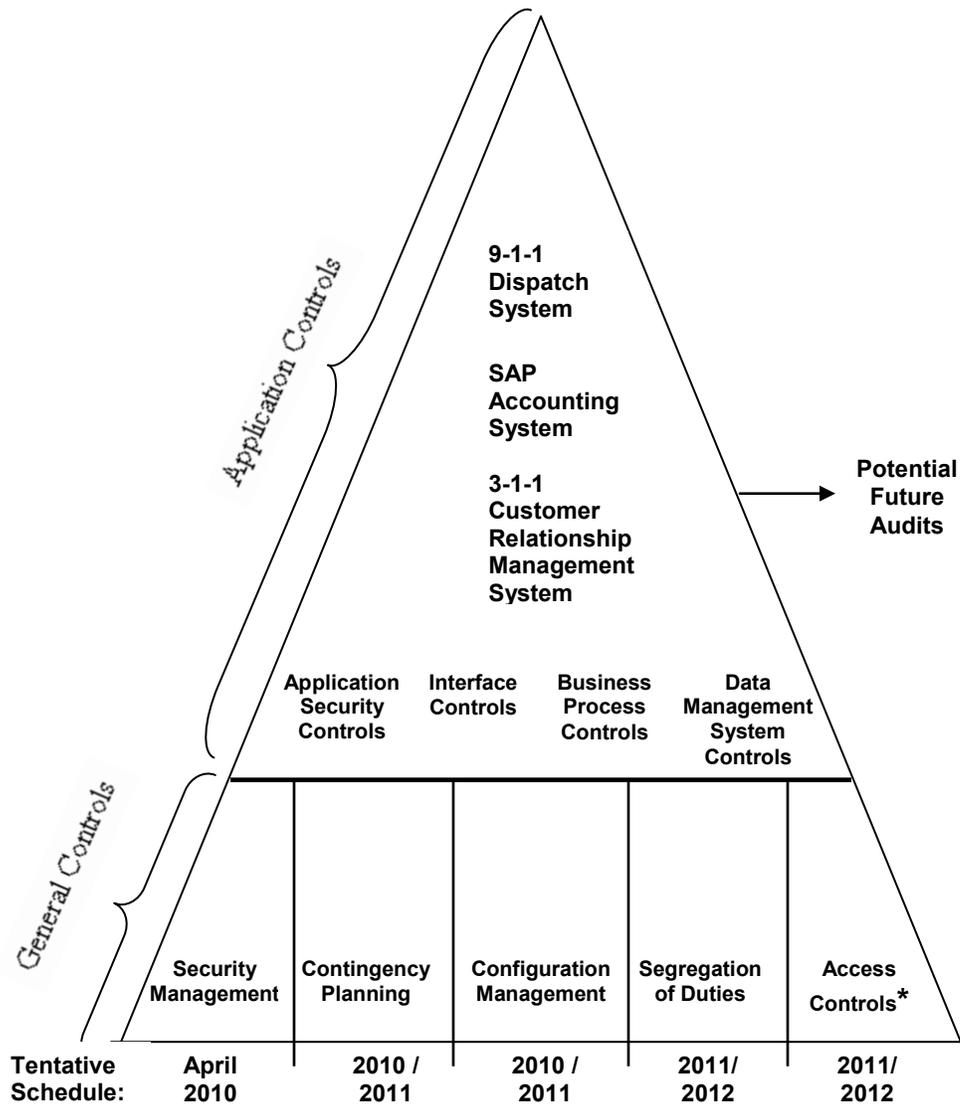
3 Defined: Management communicates consistently the need to plan for ensuring continuous service. Responsibilities are clearly defined and assigned. There is a documented IT continuity plan based on system criticality and business impact. There is periodic reporting of continuous service testing.

4 Managed and Measurable: Responsibilities and standards for continuous service are assigned and enforced. Maintenance activities are based on the results of continuous service testing, internal good practices, and the changing environment. Formal and mandatory training is provided on continuous service processes.

5 Optimized: Integrated continuous service processes take into account benchmarking and best external practices. Management ensures that a disaster or major incident will not occur as a result of a single point of failure. The IT continuity plan is integrated with business continuity plans and is routinely maintained.

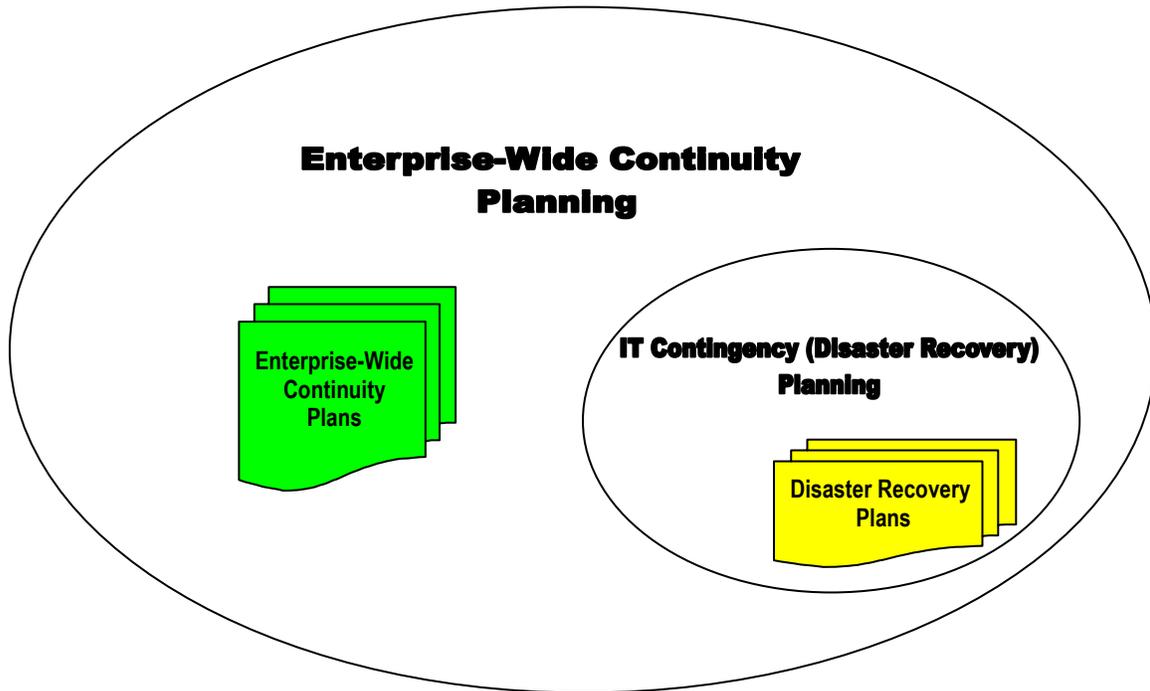
Appendix B – IT Audit Schedule

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 – Contingency, Disaster Recovery, and Continuity Planning



IT contingency (a.k.a. disaster recovery) planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency.⁹ IT contingency planning fits into a much broader emergency preparedness environment that includes enterprise-wide continuity (contingency) planning. Continuity planning provides IT and non-IT procedures for sustaining essential business operations while recovering from a significant disruption.

⁹ U.S. Government Accountability Office, *Federal Information System Controls Audit Manual* (2009), 327.

Appendix D – Staff Acknowledgement

Mark Bigler, CPA-Utah, CISA, CFE, Audit Manager
Alex Valadez, CISA, Auditor in Charge

Appendix E – Management’s Responses



CITY OF SAN ANTONIO

SAN ANTONIO TEXAS 78283-3966

February 22, 2012

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

RE: Management’s Corrective Action Plan for the IT Contingency Planning 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: COSA – Wide Contingency Plan</p> <p>Recommendation: The Chief Technology Officer should work with the City Manager’s Office to facilitate the development of a COSA-wide contingency program.</p>	4	Accept	Ben Gorzell, CFO/Hugh Miller, CTO, ITSD	03/31/2013
<p>Action plan: The City’s Emergency Operations Center (EOC) has a basic plan with annexes which document how the City’s public safety departments respond in the event of a significant emergency or natural disaster. While the City has contingencies in place for its systems and has had to execute contingency plans for its business areas (for example the fire at Riverview Towers), a single COSA-wide contingency is not documented in writing.</p> <p>The CFO and CTO will work with the EOC to facilitate the development of a Continuity Of Operations (COOP) for each of the City’s business areas. The COOP will not only address the IT contingency requirements but will also identify the approach to be utilized to allow for the continuity of business operations.</p>					

Audit of the Information Technology Services Department
IT Contingency Planning

Recommendation					
#	Description	Audit Report Page	Accept, Partially Accept, Decline	Responsible Person's Name/Title	Completion Date
B	<p>Recommendation Title: Contingency Program</p> <p>Recommendation: 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.</p>	5	Accept <i>(standalone systems outside ITSD data centers not included)</i>	Hugh Miller, CTO, ITSD	03/31/2012
<p>Action plan: Contingency Plan Program development will include a phased approach. The first phase will provide a top-down look at how ITSD provides existing services along with resources required to support them. The second and subsequent phases will provide details related to support platforms and software services that are maintained and required to meet DR requirements as agreed to between ITSD and Clients.</p> <p>Additionally, ITSD has been working with the EOC to develop an Annex to the City's emergency action plan. We contracted with UTSA ITSA's division to develop the Annex based on the State's template. The purpose of this Annex is to define the operational concepts, organizational arrangements, responsibilities, and procedures to perform a coordinated response to cyber threats and incidents. Such threats would involve the Information Technology (IT) systems and assets of the COSA which have or may have widespread impacts on the city's critical infrastructure or threaten public safety and well-being. The scope of this Annex includes threats and/or incidents that may be of a purely cyber nature, those of a physical nature that have a cyber impact, or a combination of cyber and physical impacts.</p> <p>The initial phase will be completed by 3/31/2012. The additional phase which includes developing DR plans specific to client applications hosted at ITSD will include Service Level Agreement's for each departmental client.</p>					
C	<p>Recommendation Title: Identification of Major System Applications</p> <p>Recommendation: 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.</p>	6	Accept	Hugh Miller, CTO, ITSD	04/01/2012

Audit of the Information Technology Services Department
IT Contingency Planning

Recommendation					
#	Description	Audit Report Page	Accept, Partially Accept, Decline	Responsible Person's Name/Title	Completion Date
	<p>Action plan: The ITSD Application Development and Support Division will complete an internal review of all supported major application systems in conjunction with the IT Portfolio Management office and will propose initial classification of those according to their relative importance in supporting the City's mission. That classification will then be reviewed with the business stakeholders of those systems.</p>				
D	<p>Recommendation Title: Identification of Critical/Sensitive Information Systems</p> <p>Recommendation: The Chief Technology Officer should 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.</p>	6	Accept	Hugh Miller, CTO, ITSD	05/01/2012
	<p>Action plan: ITSD will identify each application supported by each CoSA department and create a database of these applications for license tracking and DR purposes.</p> <p>A thorough business analysis will be provided by ITSD of these applications which accounts for the Total Cost of Ownership of each as well as any migration planning for platform replacement or enhancements.</p>				
E	<p>Recommendation Title: Assignment of Continuity Manager Responsibilities</p> <p>Recommendation: The Chief Technology Officer should assign continuity management responsibilities to an appropriate ITSD individual and expedite the filling of all related open IT positions.</p>	7	Accept	Hugh Miller, CTO, ITSD <i>(transition to CISO when hired)</i>	5/30/2012
	<p>Action plan: ITSD will recruit and hire CISO to lead the Security team which consists of 5 total positions within ITSD.</p> <p>CISO will recruit and fill remaining team vacancies as one of their first priorities once they join the ITSD team.</p>				

+

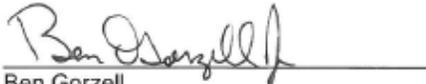
We are committed to addressing the recommendations in the audit report and the plan of actions presented above.

Sincerely,



Hugh Miller
Director
Information Technology Services Department

02/22/2012
Date



Ben Gorzell
Chief Financial Officer
City Manager's Office

2/22/2012
Date