CITY AUDITOR'S OFFICE

Disaster Recovery/Business Continuity

March 6, 2015   AUDIT REPORT NO. 1511

CITY COUNCIL
Mayor W.J. "Jim" Lane
Suzanne Klapp
Virginia Korte
Kathy Littlefield
Vice Mayor Linda Milhaven
Guy Phillips
David N. Smith

March 6, 2015

Honorable Mayor and Members of the City Council:

Enclosed is the audit report for *Disaster Recovery/Business Continuity*, which was included on the Council-approved FY 2014/15 Audit Plan. Business continuity is defined as sustaining an organization's essential functions and processes during and after a disruption. A disaster recovery plan is an information systems-focused plan designed to restore operability of systems, applications or computer infrastructure after an emergency. While several standards exist, they are all fairly consistent regarding the recommended contents of these plans.

The City Auditor's Office first conducted an audit of business resumption in 2001 and performed a follow-up audit in 2009. The 2009 audit was terminated due to lack of progress since the 2001 audit. Our current audit found that substantial progress remains to be made on the recommendations from that 2001 audit. Currently, one of the 13 recommendations has been implemented, 3 are no longer considered applicable and 9 are either not implemented or still in the process of being implemented.

Further, in addition to or in combination with its Emergency Operations Plan, the City should establish a Business Continuity Plan that incorporates a Disaster Recovery Plan.

We appreciate the assistance provided by the Fire and Information Technology departments' management and staff during this audit. If you need additional information or have any questions, please contact me at (480) 312-7867.

Sincerely,

Sharron E. Walker, CPA, CFE, CLEA
City Auditor

Audit Team:

Kyla Anderson, CIA, CLEA – Senior Auditor
Dan Spencer, CIA – Senior Auditor

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This audit of *Disaster Recovery/Business Continuity* was included on the Council-approved FY 2014/15 Audit Plan. The audit objective was to evaluate the City's risk management and preparedness for recovery from significant business interruptions. Business continuity is defined as sustaining an organization's essential functions and processes during and after a disruption. A disaster recovery plan is an information systems-focused plan designed to restore operability of systems, applications or computer infrastructure after an emergency.

In Scottsdale City Code §10-6, the City Council requires the City to have a comprehensive disaster plan. Further, the plan is intended to incorporate the services, equipment, facilities and personnel of all departments and agencies to the fullest extent.

The National Fire Protection Association defines emergency management as consisting of five elements: prevention, mitigation, preparedness, response and continuity. Disaster recovery and business continuity would fall within the preparedness and continuity activities. As well, many standard setting organizations, such as the Disaster Recovery Institute International and the International Organization for Standardization, have developed disaster recovery and business continuity standards. The various standards are closely correlated, as summarized in Table 1 of this report.

The City Auditor's Office first conducted an audit of business resumption (now called business continuity) in 2001 and performed a follow-up audit in 2009. The 2009 audit was terminated due to lack of progress since the 2001 audit. Our current audit found that substantial progress remains to be made on concerns identified in the 2001 audit. Currently, one of the 13 specific recommendations contained in the December 2001 Business Resumption audit has been implemented, with 3 no longer considered applicable and 9 either not implemented or still in the process of being implemented.

Further, additional preparation is needed to ensure essential operations continue during an emergency and normal operations can resume afterward. In addition to or in combination with its Emergency Operations Plan, the City should establish a Business Continuity Plan that incorporates a Disaster Recovery Plan. In particular, attention is needed in the following areas:

- Business Continuity Plan Management
- Business Continuity Policy, Standards and Procedures
- Risk Assessment and Business Impact Analysis
- Documentation
- Plan Training and Testing

BACKGROUND

Scottsdale City Code §10-6 requires the City to have a comprehensive disaster plan that shall be adopted and maintained by resolution. The plan is intended to incorporate the services, equipment, facilities and personnel of all departments and agencies to the fullest extent. Code §10-2 identifies the City Manager or his designated alternate as the emergency services director; this authority has been informally delegated to the Fire Chief. Within the Fire Department, the Fire Chief has established an Office of Emergency Management unit staffed with an Emergency Management Coordinator.

Regulatory and Best Practice Frameworks for Continuity Planning

Disaster recovery and business continuity planning is important preparation for the event of a major disruption caused by unexpected events, such as a terrorist attack, pandemic, fire, nuclear explosion or network virus. For example, disruption in service delivery may impact the City's ability to provide water, fire suppression, traffic control, sanitation or police services that could negatively impact the health and safety of the citizens of Scottsdale.

Federal, state and local governments have established requirements to minimize the likelihood and impact of government services being interrupted. The Federal Emergency Management Agency (FEMA) defines continuity planning as the good business practice of ensuring the execution of essential functions through all circumstances, and states that such planning is a fundamental responsibility of public institutions.[1] Arizona Revised Statutes (ARS) §26-307 provides cities the authority during a state of emergency to waive procedures otherwise required by law, such as those pertaining to public works, procurements, employing workers, using volunteers, and appropriating public funds. Further, the statute allows the governing body to take such emergency measures as deemed necessary to carry out the provisions of the emergency management law. The City Council has incorporated the powers provided in state statute into Chapter 10 of the Scottsdale City Code, along with designating powers and duties of the emergency preparedness director and other related policy.

> **Business Continuity Plan** focuses on sustaining an organization's essential business processes during and after a disruption.
>
> **Disaster Recovery Plan**, a subset of a Business Continuity Plan, focuses on information systems and is designed to restore operability of systems, applications or computer infrastructure after an emergency.
>
> **SOURCE:** NIST 800-34 Rev. 1

Many standard setting organizations have developed disaster recovery/business continuity standards and planning frameworks. Besides being very closely correlated, as shown in Table 1 on page 4, they often cross reference each other. For example, the Disaster Recovery Institute International (DRII) includes both the International Organization for Standardization (ISO standards) and National Fire Protection Association (NFPA) standards as some of its criteria, while the NFPA similarly refers to the ISO, DRII, FEMA, and others.

---

[1] FEMA is the federal agency designated to lead America to prepare for, prevent, respond to and recover from disasters.
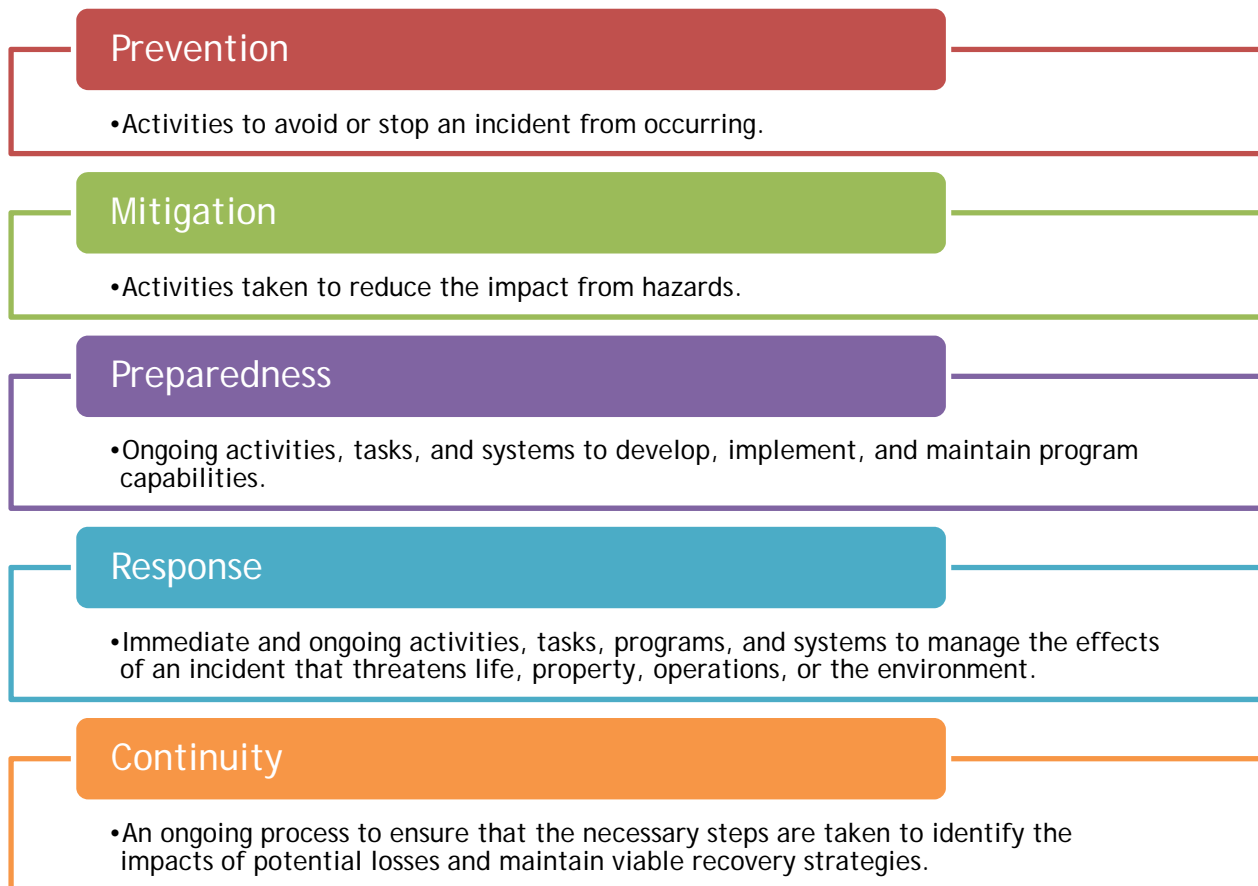
Table 1. Crosswalk of Disaster Recovery/Business Continuity Standards and Frameworks

ISACA/COBIT 4.1	DRI International	ISO 22301	NFPA 1600
Business Continuity Plan Management: The business continuity management (BCM) plan team must be organized to represent all appropriate business functions.	1. Program Initiation and Management 4. Business Continuity Strategies 9. Crisis Communication 10. Coordination with External Agencies	4. Context of the Organization 5. Leadership 7. Support	4. Program Management
Policies, Standards and Procedures: Policies affecting business continuity are implemented to ensure completeness and appropriate coverage for business risk. Policies are defined, implemented and monitored. Policies and procedures are subject to routine review to ensure they are current.	1. Program Initiation and Management 4. Business Continuity Strategies 7. Awareness and Training Programs 8. BC Plan Exercise, Audit and Maintenance	4. Context of the Organization 5. Leadership 6. Planning 7. Support 8. Operation 9. Performance Evaluation 10. Continuous Improvement	7. Training and Education 9. Program Maintenance and Improvement
Business Impact Analysis: A comprehensive Business Impact Analysis is the basis for business continuity decisions, including RTO and RPO and single points of failure.	2. Risk Evaluation and Control 3. Business Impact Analysis 5. Emergency Response and Operations 6. Plan Implementation and Documentation	4. Context of the Organization 8. Operation	5. Planning
Enterprise Risk Management: BCM is an integral component of the Enterprise Risk Management program.	1. Program Initiation and Management 2. Risk Evaluation and Control	4. Context of the Organization 5. Leadership 6. Planning 8. Operation	5. Planning
Documentation: The business continuity plan is adequately documented to conduct effective interim business activities and recovery procedures after a declared business interruption.	5. Emergency Response and Operations 6. Plan Implementation and Documentation	7. Support 8. Operation	6. Implementation
Plan Testing: The plan should be tested regularly, including a comprehensive verification of continuity processes and situational drills to test the assumptions and alternate procedures within the plan.	8. BC Plan Exercise, Audit and Maintenance	8. Operation 9. Performance Evaluation 10. Continuous Improvement	8. Exercises and Tests

SOURCE: Auditor assessment of ISACA Business Continuity Management Audit/Assurance Program, DRI International Professional Practices, ISO 22301, and NFPA 1600.

As shown in Figure 1, the NFPA defines emergency management as consisting of five types of activities: Prevention, Mitigation, Preparedness, Response and Continuity. This audit focuses on the City's Disaster Recovery and Business Continuity efforts, which fall within the Preparedness and Continuity activities of an emergency management program.

Figure 1. Five Categories of Emergency Management Activities

Prevention
- Activities to avoid or stop an incident from occurring.

Mitigation
- Activities taken to reduce the impact from hazards.

Preparedness
- Ongoing activities, tasks, and systems to develop, implement, and maintain program capabilities.

Response
- Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.

Continuity
- An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable recovery strategies.

SOURCE: Auditor review of NFPA 1600, *Standard on Disaster/Emergency Management and Business Continuity Programs*, 2013 Edition.

According to FEMA's ready.gov website, preparedness includes identifying and assessing resources, writing plans, developing a system to manage incidents and training employees so they can execute plans. The website also provides a link to download "Business Continuity Planning Suite" software developed by the Department of Homeland Security's National Protection and Programs Directorate and FEMA.

Disaster Recovery and Business Continuity Plans

Business continuity planning addresses the organization-wide business process risks and resource needs, while disaster recovery planning is more narrowly defined as addressing the underlying information technology infrastructure and business applications.

Key elements of a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP) include:

- establishing executive support

- defining program plans and procedures (roles and responsibilities)

- conducting risk assessments and business impact analyses

- identifying essential functions, services and records

- identifying interdependencies

- determining succession and/or delegation of authority

- locating alternate facilities and resources

- building the Emergency Response Team

- identifying Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)[2]

- preparing for internal and external communications during the crisis, and

- conducting regular testing, staff training, plan maintenance and auditing.

Other Facets of Incident Preparedness

In 2011, the City opened a fully equipped emergency operations center (EOC). The EOC is designed to provide a central location for all City departments responding to an emergency. The City also prepares to manage the occasional inclement weather event and recurrent special events, such as the Waste Management Phoenix Open golf tournament and Barrett-Jackson Auto Auction that bring a large number of visitors to Scottsdale annually. As necessary to manage these events, the affected departments establish a core staff in the City's EOC to coordinate activities, such as public works, police, fire, community services, and communications.

The City has an Intergovernmental Agreement (IGA) with Maricopa County for certain regional disaster and emergency services. As part of the IGA, the City pays Maricopa County approximately $12,000 annually and the County provides assistance and advisement on the development, review, publication, and distribution of the City's Emergency Operations Plan. Additionally, the County provides assistance with disaster and emergency management training and access to a comprehensive emergency management software tool, among other services.

Previous Audits

The City Auditor's Office conducted an audit of Business Resumption (now referred to as business continuity) in 2001. That audit included 13 specific recommendations to improve the City's ability to recover from a significant disruption in service. In 2009, a follow-up audit was completed to assess the status of the 2001 recommendations. That audit found that little progress had been made, and as a result was terminated.

---

[2] RTO is the maximum amount of time the organization can afford to be without a particular business process, while RPO is the point in time to which information needs to be restored. Both of these variables are based on business needs for continuing operation.

OBJECTIVES, SCOPE, AND METHODOLOGY

An audit of *Disaster Recovery/Business Continuity* was included on the City Council-approved fiscal year (FY) 2014/15 Audit Plan. The audit objective was to evaluate the City's risk management and preparedness for recovery from significant business interruptions.

To prepare for this audit, we reviewed and conducted a follow-up on the previous two audits that were conducted by the City Auditor's Office: *Business Resumption* Report No. 0162, December 20, 2001, and *Business Resumption Follow-Up* Report No. 0907, January 15, 2009.

Further, we reviewed the following:
- ISACA White Paper *Business Continuity Management: Emerging Trends* December 2012
- Disaster Recovery Institute International (DRII) Professional Practices
- International Organization for Standardization (ISO) *22301 Societal Security – Business Continuity Management Systems – Requirements*
- National Fire Protection Agency (NFPA) 1600 *Standard on Disaster/Emergency Management and Business Continuity Programs*
- National Institute of Standards and Technology (NIST) Special Publication 800-34 Rev. 1, *Contingency Planning Guide for Federal Information Systems*
- Arizona Revised Statutes Title 26, Chapter 2, Article 1 *Emergency Management*
- Scottsdale Revised Code Chapter 10 *Civil Defense and Emergency Services*
- State of Arizona Emergency Response and Recovery Plan – Basic Plan
- Maricopa County Multi-Jurisdictional Hazard Mitigation Plan
- 2007 City of Scottsdale Major Emergency Operations Plan
- Draft City of Scottsdale Emergency Operations Plan
- City of Scottsdale IT Emergency Operations Plan, Fall 2014

In addition to following-up on the findings and recommendations from the previous City Auditor reports, we used the ISACA Business Continuity Management Audit/Assurance Program to review the City's current environment. The ISACA audit program correlates to authoritative business continuity and internal control standards and frameworks as shown in Table 1 on page 4. Although ISACA is an information technology-related association, the business continuity audit program encompasses the broader business context.

This audit found that substantial progress remains to be made on concerns identified in the 2001 audit. Additionally, preparation is needed to ensure essential operations continue during an emergency and normal operations can resume afterward.

We conducted this audit in accordance with generally accepted government auditing standards, as required by Article III, Scottsdale Revised Code §2-117 et seq. 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 work took place from November 2014 to February 2015.

FINDINGS AND ANALYSIS

1. Substantial progress remains to be made on concerns identified in the 2001 audit.

Although 13 years have passed since the City Auditor's first business resumption audit and 6 years since the audit follow-up, there has been little progress made. The December 2001 audit report identified an overall issue of the City not having a business resumption planning program (now referred to as business continuity), and the 2009 follow-up review found little progress. Currently, of the 13 specific recommendations contained in the December 2001 business resumption audit, 1 recommendation was implemented, 3 are no longer applicable and 9 have not been implemented or are still in the process of being implemented. The recommendations that have not been implemented or remain in progress, along with their current status, are summarized in Table 2.

Table 2. Status of 2001 Audit Recommendations

Recommendation	Status	Description
Develop a business resumption *(now business continuity)* plan that defines the responsibilities, roles, and approval process for the plan. The plan should be based on a risk assessment and impact analysis. *(The recommendation also listed minimum content requirements for the plan.)*	Not Implemented	
Require each business unit to establish responsibility for plan development, activation and maintenance. In addition, the Emergency Services Director should assume responsibility for ensuring that departmental plans are current, sufficient and supplemental to the citywide plan.	Partially Implemented	In 2009, all departments were asked to update their business continuity plans. However, departmental plans are not reviewed by Emergency Management staff to ensure they remain current, sufficient and supplement the Citywide plan. Some departments maintain their plans on an ongoing basis, such as the IT department and the Water Resources Division. These plans are not reviewed by Emergency Management staff.
Ensure the City's Risk Management Director participates in the development of the Citywide plan.	Not Implemented	
Hold a formal meeting after each incident or successful resumption to review recovery procedures and modify the plan, if necessary.	Not Implemented	The Emergency Operations Plan (EOP) has been tested and after-incident meetings held several times, but these exercises have been focused on emergency response rather than larger-scale business continuity.

Recommendation	Status	Description
Develop and implement an annual training program to ensure that employees are aware of specific requirements.	Not Implemented	
Keep the City's Emergency Response Plan current, particularly when there are organizational changes. The ERP had not been updated since 1998.	In Progress	The City's current EOP was approved by City Council in 2007, but has not been updated since. A currently existing draft EOP update has not been completed or approved.
Complete an enterprise-wide risk assessment of all applications using the City's network or supported by IT to determine minimum acceptable time for recovery of the City's network and/or server farm.	In Progress	IT is currently updating its inventory of all City applications focused on identifying critical applications. Step two will classify other non-critical applications based upon Recovery Time Objectives.
Develop a best case scenario regarding the time to provide service should the IT department's main building become inaccessible or sustain damage that impacts portions of the computer network.	In Progress	In October 2014, the IT department engaged an outside consultant to critique a plan developed by IT staff as well as to estimate plan implementation costs.
Create an alternative computer operations center and develop strategic plans for bringing that site online, if necessary.	In Progress	The City still does not have an alternate computing site. IT has recently engaged an outside consultant to critique a plan developed by IT staff as well as to estimate plan implementation costs.

SOURCE: Auditor review of management status of *Business Resumption Report No. 0162* recommendations.

By completing and maintaining the business continuity and disaster recovery plans, City staff can more fully comply with the City Council's policy direction to develop and maintain by resolution a comprehensive emergency services/disaster plan.

Recommendation:

The City Manager should require Emergency Management and Information Technology staff to complete the City's business continuity and disaster recovery plans to address the remaining recommendations in Table 2. Further, once completed, staff should be required to ensure the plans are updated regularly.

2. **Additional preparation is needed to ensure essential operations continue during an emergency and normal operations can resume afterward.**

The City is required to develop an Emergency Operations Plan (EOP) in support of the State of Arizona Emergency Response and Recovery Plan (SERRP) and the Maricopa County Emergency Operations Plan. The Maricopa County Department of Emergency Management provides a boilerplate EOP that the City Emergency Management staff customizes. The City Council last reviewed and approved the City's EOP in 2007; however, the Emergency Management Coordinator currently is working on an updated draft document.

The City's EOP is required to provide an overview of the City's Emergency Management structure and the various City departments assigned to certain responsibilities in the event of a major emergency. While related, a Business Continuity Plan (BCP) outlines the resource requirements for the City to maintain essential day-to-day operations as well as effectively and efficiently responding to the emergency.[3] In particular, attention is needed in the following areas.

- **Business Continuity Plan Management**
  To be effective, the business continuity plan should be managed by a team that represents all City business functions and areas and involves the City's senior management staff with a global perspective of their departments.

  Currently, the citywide Emergency Safety and Preparedness group (ESAP) represents a cross-section of business functions, but only includes 2 to 3 members of senior management. Based on sign-in sheets, the senior management members generally do not attend ESAP meetings.

  The team leader should report to a senior executive with cross-organizational responsibilities, such as the City Manager. The current Emergency Management unit is within the Fire Department, making the resources more susceptible to departmental priorities.

- **Business Continuity Policy, Standards and Procedures**
  Policies and procedures for business continuity are needed to ensure that continuity planning occurs and provides complete and appropriate coverage for business risks. In addition, the program should be based upon recognized standards or frameworks, such as those listed in Table 1 on page 4.

- **Risk Assessment and Business Impact Analysis (BIA)**
  Risk assessment is the process of identifying hazards and analyzing probabilities, vulnerabilities, and impacts. Identified risks should be included in the BIA.

  The BIA is a management level analysis that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an entity's resources. In particular, the BIA includes a detailed analysis of all single points of failure in the business functions and areas.

  Additionally, a defined BIA methodology should be implemented, and the BIA should be updated at least annually by the business and support units.

  An effective risk assessment and BIA process helps ensure the City's business continuity plan is complete and addresses the most significant entitywide risks.

- **Documentation**
  Although the existing draft EOP references a Continuity of Operations Plan (or BCP), that plan has not been prepared. In mid-2009, City departments were requested to submit departmental emergency response plans, but these individual plans were not incorporated into a coordinated citywide plan. The current Emergency Management Coordinator stated that each City department is responsible for creating and maintaining its own BCP.

---

[3] At times, the Business Continuity Plan is referred to as a Continuity of Operations Plan (COOP) or Continuity of Government Plan (COG).

A business continuity plan should be adequately documented and available during a declared emergency to facilitate effective interim business activities and recovery procedures. Further, to be useful, the plan should be kept current and reflect changes in:

- business processes
- operating environment
- technology
- third-party relationships
- relevant contracts
- regulatory and other compliance requirements

- **Plan Training and Testing**
  Training and testing is a necessary component of business continuity preparedness. The Emergency Management Coordinator attended classes providing 130 continuing education hours in 2014 and 355 hours in 2013, but most of the training related to executive leadership and incident management rather than business continuity plan management. Further, senior City staff who would most likely be key participants in the event of a significant event should be trained on the BCP.

  While the existing draft EOP assigns responsibilities to City departments, the draft has not been circulated for feedback and agreement. In the event of an emergency, departments will not be familiar with expectations defined in the EOP.

  To test the assumptions and alternate procedures within the plan, the BCP should be tested regularly, and the tests should include a comprehensive verification of continuity processes and situational drills. Test results should then be analyzed to identify issues that may require BCP revisions, additional training or additional resources.

Recommendation:

The City Manager should require the Emergency Management staff to ensure City departments review and update their BCPs annually or whenever there has been a significant organizational change. Also, Emergency Management staff should review them to ensure the departmental plans are based on risk assessment and business impact analysis. After review, Emergency Management staff should incorporate the departmental BCPs into the citywide BCP and ensure they are periodically tested.

MANAGEMENT ACTION PLAN

1. Substantial progress remains to be made on concerns identified in the 2001 audit.

Recommendation:

The City Manager should require Emergency Management and Information Technology staff to complete the City's business continuity and disaster recovery plans to address the remaining recommendations in Table 2. Further, once completed, staff should be required to ensure the plans are updated regularly.

<u>Emergency Management</u>

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: Management agrees with the need for comprehensive business continuity (BC) and recovery plans as they are part of an overall disaster management process. The 2015 Audit confirmed that the City of Scottsdale's BC plan has been in the ideation phase for the past fourteen years. In 2008 this finding was identified as a result of the staffing and budget deficiencies and the lack of a centralized organization of Emergency Management. The revision of the City's Emergency Operation Plan will assist in outlining roles and responsibilities of City business units however leadership support will be required to implement City Code changes, Department Leadership job requirements and support of an Emergency Management Steering Group.

RESPONSIBLE PARTY: Emergency Management Officer

COMPLETED BY: 7/1/2015

<u>Information Technology</u>

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: Information Technology staff will work with its business partners to further define recovery time objectives beyond those systems that have been deemed critical to the City.

Information Technology is currently working with an outside consultant to present a recommended approach, location and cost to restore City service should the City's main datacenter become inaccessible. The plan will include two alternatives. The first will be to restore critical City services and the second will be to recover all City services.

RESPONSIBLE PARTY: Shannon Tolle

COMPLETED BY: 1/8/2016

2. Additional preparation is needed to ensure essential operations continue during an emergency and normal operations can resume afterward.

Recommendation:

The City Manager should require the Emergency Management staff to ensure City departments review and update their BCPs annually or whenever there has been a significant organizational change. Also, Emergency Management staff should review them to ensure the departmental plans are based on risk assessment and business impact analysis. After review, Emergency Management staff should incorporate the departmental BCPs into the citywide BCP and ensure they are periodically tested.

MANAGEMENT RESPONSE: Agree

PROPOSED RESOLUTION: Management agrees leadership should ensure yearly review of expectations that City departments update and semiannually test their respective BC plans. The review should include a review of the BCP, a performance test of the BCP in the department, and should involve one third of department personnel (for the purpose of institutionalizing and enculturating the BCP process). Lessons learned of testing should be forwarded to Emergency Management and City Manager for review. Emergency Management should be required to annually review and validate sufficiency of the plans along with a review of the risks identified.

RESPONSIBLE PARTY: Emergency Management Officer

COMPLETED BY: 7/1/2015

The City Auditor's Office conducts audits to promote operational efficiency, effectiveness, accountability, and integrity.