MANAGEMENT AUDIT REPORT

OF

DISASTER RECOVERY PLAN
DEPARTMENT OF FINANCE AND ADMINISTRATIVE SERVICES
INFORMATION TECHNOLOGY SERVICES DIVISION

REPORT NO. 13-101

City of Albuquerque
Office of Internal Audit

Department of Finance and Administrative Services – Information Technology Services Division
Disaster Recovery Plan
Report No. 13-101
Executive Summary

The Office of Internal Audit (OIA) conducted a management audit of the Disaster Recovery (DR) Plan prepared by the Information Technology Services Division (ITSD), a division of the Department of Finance and Administrative Services (DFAS). The audit was included in the fiscal year (FY) 2013 approved audit plan.

Having a current and reliable DR Plan is a necessity for all municipal governments. A well-designed DR Plan is a tool for ensuring that required technology is available on an ongoing basis. Although a plan cannot anticipate all potential threats, DR planning provides a framework for managing the disruption through damage assessment and activation of recovery processes when the unexpected occurs.

ITSD's current DR Plan was completed in February, 2012. This version of the plan was a complete re-write of previous DR plans and was based on City-wide critical IT needs. ITSD utilizes a layered approach to prevent data loss. For critical systems, the first line of defense is redundancy. Redundant systems located at hot sites provide failover capability. Secondary protection is provided through daily performance of backups to external media.

The DR Plan is currently undergoing testing through a series of User Acceptance Tests (UATs). Each test is designed to test a specific recovery procedure. If any part of a test fails, the methodology calls for re-testing to ensure that recovery steps will be successful in an emergency.

Does the Disaster Recovery Plan permit ITSD to sufficiently recover critical IT systems to allow City Departments to resume normal functions after a disruption?

- ITSD has not obtained step-by-step recovery procedures from three City departments describing services to be provided by ITSD in an emergency. The lack of detail may negatively impact recovery efforts or interrupt availability of critical services required by external departments.

- Two servers that support Tier 1 internal service priorities are located at the secondary hot site, which is limited to approximately 45 minutes of backup electricity if utility power is unavailable. Should an electrical outage exceeding 45 minutes occur, these servers would not be available for failover.

- A division-specific emergency purchasing procedure does not currently exist. Should a large dollar server or component require replacement, ITSD may not be able to acquire the required equipment in a timely fashion.

- Due to employee retirements, transfers and resignations, the DR Plan contact information was outdated at the time the audit began. In a disaster scenario, the lack of current contact information may delay the assembly of an appropriate recovery team.

- The maintenance interval for updating the DR Plan has not been formally established. Without ongoing DR plan updates, recovery of essential systems may be delayed or outdated recovery steps may be attempted.

Have backup and recovery procedures been established and tested to ensure availability of data?

ITSD does not currently perform formal tests of recovery from backup media. Should a disaster necessitate recovery from backup, restoration of critical services may be delayed beyond the 24-hour recovery time objective.

Is the Disaster Recovery Plan tested regularly to ensure that key IT systems can be effectively recovered?

Current DR Plan testing does not consider the unexpected. Without periodic drills, recovery personnel may lack preparation to quickly execute recovery procedures under unusual or unforeseen circumstances.

Recommendations and management responses are included in the audit report.

City of Albuquerque

Office of Internal Audit

P.O. BOX 1293 ALBUQUERQUE, NEW MEXICO 87103

February 27, 2013

Accountability in Government Oversight Committee
City of Albuquerque
Albuquerque, New Mexico

Audit: Management Audit
Department of Finance & Administrative Services
Information Technology Services Division
Disaster Recovery Plan
Audit No. 13-101

FINAL

INTRODUCTION

The Office of Internal Audit (OIA) conducted a management audit of the Disaster Recovery (DR) Plan prepared by the Information Technology Services Division (ITSD), a division of the Department of Finance and Administrative Services (DFAS). The audit was included in the fiscal year (FY) 2013 approved audit plan.

Having a current and reliable DR Plan is a necessity for all municipal governments. A well-designed DR Plan is a tool for ensuring that required technology is available on an ongoing basis. Although a plan cannot anticipate all potential threats, DR planning provides a framework for managing the disruption through damage assessment and activation of recovery processes when the unexpected occurs.

Key terms utilized in this report:

- Business continuity plans (BCPs) – Enterprise-wide sets of plans used by departmental units to respond to a disruption in order to recover standard business processes. City-wide BCPs are outside the scope of this audit.

- Business Impact Analysis (BIA) – An enterprise-wide process utilized to determine an organization's most critical business processes and identify the underlying IT systems and applications needed to support such processes.

- CobiT – An internationally accepted process framework for IT that provides a comprehensive IT governance, management, control, and assurance model. CobiT objectives support enterprises in the development, implementation, and continuous improvement and monitoring of good IT-related governance and management practices.

- Disaster Recovery Plan – DR Plans are a subset of BCPs. These are the plans and procedures for recovering key information technology infrastructure critical to the organization, as determined by a BIA.

- Hot site – A hot site is an offsite datacenter equipped with replicas of critical IT infrastructure. A hot site can take the place of the principal datacenter in the event of a disaster or disruption.

- Redundancy – Replication of key IT components at a hot site, permitting fast recovery of critical IT infrastructure.

- Failover – The ability to transfer a key IT service from the principal datacenter to a redundant system at a hot site. Failover may be executed automatically or manually by following a set of DR procedures.

- Backup Media – Electronic copies of system, application software, and related databases which can be utilized to restore applications and databases in the event the originals are lost or destroyed.

- Tabletop exercise - A mock disaster exercise designed to test the IT function's knowledge of recovery plans and assess the ability of recovery teams to respond to a hypothetical disaster scenario or scenarios.

Key documents evaluated in this audit:

Disaster Recovery Plan, Tier 1 City of Albuquerque Critical Services, February 23, 2012 (Revision 1)

This is ITSD's principal DR Plan document and the central focus of the audit. The document was developed by a contractor in fiscal year 2012 and supersedes previous DR plans developed by ITSD. The intention of the current plan is to address emergency responses to outages of IT infrastructure and services critical to City departments.

Identification of critical IT functions was based on a lengthy process of interaction with City departments and divisions which resulted in a City-wide Business Impact Analysis (BIA). The goal of the BIA was to ensure that the new DR plan would be aligned with the critical IT needs of the City, as identified by the technology users. Based on analysis of the BIA, ITSD determined the top five critical service groups: Police, Fire, Transit, 311, and Animal Welfare. Identification of the top five service groups determined which Tier 1 critical services, internal services, and applications would be recovered first in a disaster scenario.

The DR Plan is designed to recover critical service functions of the City. Based on the BIA, critical service functions were ranked into four tiers, with Tier 1 having the greatest criticality. Following recovery of Tier 1 utilities, internal services, and applications, Tiers 2 through 4 are recovered, in that order, if resources are available.

The mission of the DR Plan is "to determine the critical service functions of the City that have an IT component which is supported by the ITSD; develop a strategy to prioritize and recover the IT components of these critical functions; and finally, to develop a maintenance and validation process for the Disaster Recovery Plan." The DR Plan has three phases:

1. Planning and Project Initiation,
2. Develop DR Strategies, and
3. Establish maintenance and validation of the DR Plan.

The first two phases were completed prior to commencement of this audit. The first phase included defining objectives, identifying critical functions of the City which have IT components supported by the ITSD, and compiling results into a BIA. Phase two focused on developing recovery procedures and gaining management approval of DR plan documents. The third phase relates to ongoing testing and validation of the plan, as well as updating the plan. The original contract called for preparation and delivery of the initial documents. Therefore, phase three is open-ended and calls for ITSD to implement this phase. Because phase three is still in process, the audit only evaluated progress to date. Some audit recommendations address future revisions of the DR plan.

Other DR Plan Documentation

There are several companion documents to the DR Plan, which serve as the roadmap for the Chief Information Officer or designee to follow during a disaster declaration. These

documents outline operational and physical requirements of various disaster scenarios. These documents are intended to provide detailed procedures for recovering Tier 1 critical utilities, internal services, and applications as determined by the BIA. They also contain recovery instructions for some Tier 2 priorities, which would be recovered after restoring the Tier 1 priorities.

Documentation includes initial procedures for the Disaster Assessment Team to assess the damage to the systems and notify personnel who will be recovering the systems. Damage assessment determines the type of recovery to be performed. The City has four recovery classes, which are outlined below:

- Class 1 Recovery – Equipment is not functioning and must be recovered in an alternate location with new or alternate equipment.
- Class 2 Recovery – Equipment is not functioning, but can be recovered in place with new or alternate equipment.
- Class 3 Recovery – Equipment is functioning, but must be removed and installed in an alternate location.
- Class 4 Recovery – Equipment is functioning and can remain in place.

Once the type of recovery has been determined, appropriate recovery teams are assembled to activate the recovery procedures. The DR Plan is designed to simultaneously recover critical utilities, internal services, and applications. The plan can also be utilized to recover individual systems, services, or applications should there be an isolated disruption.

For example, one set of recovery instructions for a Tier 2 application were activated during the fieldwork phase of the audit. On a November 2012 weekend, a hardware failure necessitated activating the plan to recover a Human Resources database in the City's Enterprise Resource Planning (ERP) system. The response by on-call ITSD personnel was a successful failover to the DR hot site with minimal downtime and no data loss. Temporary workarounds were devised and the DR server was utilized in place of the production server for approximately three weeks. This unplanned emergency underscores the importance of well-designed and documented recovery procedures for critical applications.

AUDIT OBJECTIVES

The objectives of the audit were to determine:

- Does the Disaster Recovery Plan permit ITSD to sufficiently recover critical IT systems to allow City Departments to resume normal functions after a disruption?
- Have backup and recovery procedures been established and tested to ensure availability of critical data?
- Is the Disaster Recovery Plan tested regularly to ensure that critical IT systems can be effectively recovered?

SCOPE

Our audit did not include an examination of all functions and activities related to the ITSD DR Plan. The scope of this audit was limited to review of DR Plan documents developed by ITSD. Documentation was assessed for conformance to practices established by Control Objectives for Information and related Technology (CobiT) and internally-established ITSD objectives and standards. This audit was not intended to be an assessment of City-wide business continuity plans, which are the responsibility of individual City departments.

The scope included examination of preventive strategies, such as redundant power, replication of applications and data and provisioning of alternate sites, and an in-depth review of plan documents. The scope also included routine backup and recovery strategies employed by ITSD to ensure availability of data.

This report and its conclusions are based on information taken from a sample of transactions and do not intend to represent an examination of all related transactions and activities. The audit report is based on our examination of activities through the completion of fieldwork, December 12, 2012, and does not reflect events or accounting entries after that date. Because phase three of the DR Plan is still in process, the audit only evaluated progress to date. Some audit recommendations address future revisions of the DR plan.

We conducted this management 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.

METHODOLOGY

To achieve the audit objectives, several methodologies were utilized. The methodologies included the following:

- In-depth review of primary and secondary plan documents, including:
    - Disaster Recovery Plan, Tier 1 City of Albuquerque Critical Services, February 23, 2012 (Revision 1),
    - System-specific disaster recovery documents available to ITSD personnel, and
    - Run books, Test Readiness Reviews (TRRs), and plans used for testing individual plan components.
- Corroboration of documentary evidence through interviews with ITSD personnel, walkthroughs of ITSD facilities, and observations of actual recovery tests
- Review of on-site physical security at main datacenters and hot sites
- Physical inspection of datacenters to verify server locations denoted in recovery plans
- Testing of contact lists to verify current employment of recovery personnel and accuracy of contact information
- Review of backup job completion notices for two calendar weeks
- Observation of transport of backup media to offsite locations
- Datacenter walkthroughs to physically locate backup hardware and tape storage facilities

FINDINGS

The following findings concern areas that we believe could be improved by the implementation of the related recommendations.

1. DFAS, ITSD SHOULD UPDATE DR RECOVERY PROCEDURES TO INCLUDE INSTRUCTIONS FOR RECOVERING ALL TIER 1 CRITICAL UTILITIES, INTERNAL SERVICES, AND APPLICATIONS.

   ITSD has not obtained step-by-step recovery procedures from three City departments describing services to be provided by ITSD in an emergency. Principal support for some Tier 1 components is the responsibility of City departments with independent IT support organizations. ITSD is responsible for providing hot site support for these Tier 1 components. Servers and other equipment are in place at designated hot sites; however, the DR plan documentation does not clearly state failover procedures. The lack of detail may negatively

impact recovery efforts or interrupt availability of critical services required by external departments.

The DR Plan Mission Statement calls for ITSD to "determine the critical service functions of the City that have an IT component which is supported by the ITSD" and "develop a strategy to prioritize and recover the IT components of these critical functions."

RECOMMENDATION

DFAS, ITSD should:

- Update the DR Plan documentation to include recovery instructions for all Tier 1 applications.
- Work with other City departments to obtain recovery steps for applications that failover to the main datacenter.
- Ensure that plan documentation contains current hardware requirements, physical locations of the underlying systems, and contact information for system administrators.

RESPONSE FROM DFAS - ITSD

"ITSD is in the process of creating the recovery procedures for all tier 1 applications and will have the responsible department review and approve content. These will be in the next version of the DR Plan documentation.

"The current hardware requirements, physical locations of the underlying systems, and contact information for system administrators is being updated for the next DR Plan version and will be completed annually."

ESTIMATED COMPLETION DATE

"April 2013."

2. DFAS, ITSD SHOULD ENSURE THAT ALL TIER 1 SYSTEMS ARE PROTECTED FROM AN EXTENDED ELECTRICAL OUTAGE.

Two servers that support Tier 1 internal service priorities are located at the secondary hot site, which is equipped with backup electricity from uninterruptible power supply (UPS) sources. The UPS units can provide approximately 45 minutes of electricity if utility power is

unavailable. Other hot sites are supported by UPS power plus diesel generators, which can continue to provide electricity significantly beyond the capacities of the UPS units. Until recently, ITSD had limited space at the primary hot site, which was shared with another agency. The secondary site was initially designed as a backup facility for a Tier 2 application. Because this was not the production facility, UPS power was considered adequate. Should an electrical outage exceeding 45 minutes occur, these servers would not be available for failover. The DR Plan's risk assessment concluded that the greatest threat to continuity of operations was an extended electrical outage.

RECOMMENDATION

DFAS, ITSD should relocate servers supporting Tier 1 critical services, internal services and applications from the secondary to the primary hot site.

RESPONSE FROM DFAS - ITSD

"The current environments (DNS, DHCP, ERP) at the secondary DR site are secondary fail-over environments that are replicated real time. The reason for this redundancy is to minimize outages and provide instant recovery to these systems. Today since they are secondary fail-over systems we do not consider the power as a high risk issue but it is something we can do to make it even more fail safe.

"ITSD will plan to migrate the systems to the primary DR site with the backup generator."

ESTIMATED COMPLETION DATE

"October 2013."

3. DFAS, ITSD SHOULD DEVELOP AN EMERGENCY PURCHASING PROCEDURE TO EXPEDITE ACQUISITION OF NEW OR ALTERNATE EQUIPMENT WHEN REQUIRED FOR A CLASS 1 OR CLASS 2 RECOVERY.

A division-specific emergency purchasing procedure does not currently exist. Provisions have been made for incidental after-hours purchases of hardware or software, but these are restricted to standard purchasing card limits. These constraints may impede the acquisition of new or alternate equipment within stated recovery time frames. Should a large dollar server

or component require replacement, ITSD may not be able to acquire the required equipment in a timely fashion.

DR Plan documentation contains the expectation that "after a disaster, critical systems and data must be recovered and operational within 24 hours, and the data recovered must be less than 24 hours old." If a recovery determination indicates a Class 1 or Class 2 recovery, the acquisition of new or alternate equipment may be required. Without an emergency purchasing procedure, the 24-hour recovery time frame may not be achievable.

RECOMMENDATION

DFAS, ITSD should:

- Develop an emergency procurement procedure to expedite purchases of IT equipment in the event of a disaster declaration.
- Define conditions under which the procedure is activated.

RESPONSE FROM DFAS - ITSD

"ITSD will use the Emergency Procurement procedure 10.7.3 in the Purchasing Rules and Regulations document that allows the department director to authorize purchases in case of an emergency. We will add a section to the current DR Plan to document the current and proposed emergency purchasing procedure and identify when it will be activated and who will be authorized to execute it in case the department director is not available."

ESTIMATED COMPLETION DATE

"April 2013."

4. DFAS, ITSD SHOULD UPDATE RECOVERY TEAM CONTACT INFORMATION ON A QUARTERLY BASIS AND UPDATE DR PLAN DOCUMENTATION.

Due to employee retirements, transfers and resignations, the DR Plan contact information was outdated by the time the audit began in October 2012. Of 28 names listed on the ITSD Disaster Team Organization Chart, two had retired, one had transferred, and two had resigned. These former employees were also listed on the contact list included as Appendix

IV in the DR Plan. This information was current when plan documentation was first published in February 2012. However, ITSD didn't revise the organization chart and contact list after personnel changes. The plan maintenance scheme and schedule have not yet been formally defined.

Successful recovery of IT infrastructure is dependent on rapid assembly and deployment of ITSD personnel. DR Plan documentation includes an Organization Chart, indicating DR roles and responsibilities, and a contact list for recovery personnel. In a disaster scenario, the lack of current contact information may delay the assembly of an appropriate recovery team. This condition was brought to the attention of ITSD management, who prepared an updated DR Organizational Chart and contact list during the audit.

Phase three of the DR Mission Statement calls for ITSD to "define a plan maintenance scheme and schedule." CobiT control objectives stress the importance of timely communication of changes in procedures and personnel relating to DR plans. Because organizational personnel changes can occur at any time, it is vital that responsibilities and contact information in DR Plan documentation contain current and accurate information in order to efficiently locate and assemble recovery personnel in a disaster.

RECOMMENDATION

DFAS, ITSD should implement a quarterly review of the ITSD Disaster Recovery Organization Chart and ITSD Contact Lists for Disaster Recovery. The review process should analyze recovery team responsibilities that may have changed as well as contacting recovery team members to verify accuracy of contact information.

RESPONSE FROM DFAS - ITSD

"The current proposed update for the DR Plan is annual, but quarterly updates to the contact information will be completed. We will add a requirement to update this section quarterly."

ESTIMATED COMPLETION DATE

"April 2013."

5. DFAS, ITSD SHOULD PERIODICALLY TEST EMERGENCY MANAGEMENT TEAM READINESS THROUGH TABLETOP EXERCISES.

Current DR Plan testing does not consider the unexpected. There is not currently a mechanism for stress-testing the plan and assessing team readiness in unannounced situations.

The current testing cycle calls for a series of User Acceptance Tests (UATs) to test each of the Tier 1 critical services, internal services, and applications. This testing phase began in spring 2012 and is not yet complete. While this type of testing is critical to testing recoverability of key systems, it is performed on a scheduled basis by system experts. Testing should also consider whether recovery procedures can be successfully executed by alternate personnel and assess the readiness of emergency management team personnel. Without periodic drills, recovery personnel may lack preparation to quickly execute recovery procedures under unusual or unforeseen circumstances.

Phase three of the DR Plan calls for DFAS, ITSD to "Establish maintenance and validation of the Disaster Recovery Plan" and to "train the Emergency Management Team on components and requirements of an exercise program." CobiT recommends integrated testing scenarios to keep DR plans relevant. Although it is not possible to anticipate all disaster scenarios, a tabletop exercise is a cost-effective way of testing the emergency management team's ability to react to unplanned events without the interruption of a full-scale drill. Such exercises can also test the recovery plan's assumptions and may identify outdated or incomplete sections of the plan.

RECOMMENDATION

DFAS, ITSD should periodically test the emergency management team's ability to adapt to unplanned situations by conducting tabletop exercises and/or recovery drills. Training sessions should present recovery personnel with previously unannounced hypothetical disasters and challenge the team to develop an appropriate recovery plan based on the current DR documentation and team knowledge.

RESPONSE FROM DFAS - ITSD

"Table top testing will be added to the DR Plan and be used as a training aide for critical recovery personnel."

ESTIMATED COMPLETION DATE

"April 2013."

6. DFAS, ITSD SHOULD PERIODICALLY TEST ITS ABILITY TO RECOVER TIER 1 SERVERS, APPLICATIONS, AND DATA FROM BACKUP MEDIA.

DFAS, ITSD does not currently perform formal tests of recovery from backup media. The division routinely performs restoration of data files and folders and is confident in its ability to restore from archived media. For DR purposes, tape backups are considered the secondary means of recovering Tier 1 infrastructure and applications and would only be necessitated in the event a failover component was unavailable. Because extreme disaster scenarios may require recovery from backup media, emergency management teams need to be prepared for such a possibility.

Without formal recovery testing, recovery personnel may not be able to timely recover Tier 1 components. Restoration of critical services may be delayed beyond the 24-hour recovery time objective.

CobiT standards recommend periodic tests of archived data. Regular testing of recovery procedures helps ensure that recovery personnel can successfully recover these Tier 1 components if needed in a disaster.

RECOMMENDATION

DFAS, ITSD should schedule a recovery test from backup media annually. Testing should be formally documented and have a predetermined objective. The test should verify the integrity of backup media by restoring an entire server or entire application and related databases from archived backups. The restored media should be compared against the production system to ensure functionality and verify data integrity.

RESPONSE FROM DFAS - ITSD

"Backup recoveries are performed almost daily by the systems and database groups, but we will add this to the testing requirements, create a Test Readiness Review (TRR) document, test plan, and then schedule for testing."

ESTIMATED COMPLETION DATE

"April 2013."

7. DFAS, ITSD SHOULD ANNUALLY REVIEW AND UPDATE THE DR PLAN TO ENSURE THAT DOCUMENTATION REMAINS CURRENT.

The initial DR Plan documents were created by a contractor, with no definite arrangements for future updates. At the time of the audit, this maintenance interval had not yet been defined. Phase three of the DR Plan calls for ITSD to define a plan maintenance scheme and schedule. CobiT standards emphasize the necessity of keeping DR plans current, to reflect changes in business processes and systems.

Technology infrastructure, systems and support procedures change over time. Without ongoing DR plan updates, recovery of essential systems may be delayed, or outdated recovery steps may be attempted.

RECOMMENDATION

DFAS, ITSD should:

- Review and update DR plan documentation on an annual basis.
- Updates should incorporate changes in underlying systems and recovery procedures.
- Include a reassessment of the critical applications list and recovery sequence in the annual review.
- State the maintenance interval standards in future versions of the DR Plan.

RESPONSE FROM DFAS - ITSD

"ITSD has scheduled an annual review for the DR documentation scheduled for March and April 2013. Although it was not documented in the DR Plan, ITSD will add sections for DR updates, incorporate changes in underlying systems and recovery procedures, critical application list and recovery sequences, state maintenance interval standards, and add them to the next release scheduled for April 2013."

ESTIMATED COMPLETION DATE

"April 2013."

CONCLUSION

We believe this audit will assist the DFAS, Information Technology Services Division improve its DR planning efforts and enhance the department's ability to ensure continuous service of critical IT components.

We appreciate the assistance and cooperation of DFAS, Information Technology Services Division personnel during the audit.

_____
Senior Information Systems Auditor

REVIEWED and APPROVED:

_____
Carmen Kavelman, CPA, CISA, CGAP, CFE
Director, Office of Internal Audit

APPROVED FOR PUBLICATION**:**

_____
Chairperson, Accountability in
Government Oversight Committee