Metropolitan Transportation Authority
One Gateway Plaza
Los Angeles, CA 90012-2952
213.922.2000 Tel
metro.net

Metro

June 1, 2006

TO: BOARD OF DIRECTORS

THROUGH: ROGER SNOBLE
CHIEF EXECUTIVE OFFICER

FROM: RUTHE HOLDEN
MANAGING DIRECTOR, MANAGEMENT AUDIT SERVICES

SUBJECT: FINAL AUDIT REPORT ON INFORMATION TECHNOLOGY SERVICES DISASTER RECOVERY PLAN

Issue

Management Audit Services (MAS) conducted an audit of the Information Technology Services (ITS) Emergency Response/Information Technology Recovery Plan (DRP) to verify whether the DRP is current, adequate, and effective to ensure the continuity of operations.

The DRP was developed to restore data processing services in the event of a disruption. The objective of the DRP is to identify and document mission critical processes and procedures to easily and quickly respond and recover from emergency and/or disaster impacts within 72 hours. ITS conducts tests of these mission critical systems on a semi-annual basis to determine whether the DRP is effective.

Scope

The scope of the audit included a review of the DRP and an assessment of the scheduled testing conducted on July 2005. The audit did not include the Supervisory Control and Data Acquisition (SCADA) DRP, Advanced Transportation Management System (ATMS) DRP and the Emergency Preparedness Plan (EPP).

Finding

72-Hour Recovery Goal for All Mission Critical Systems Never Tested

ITS has not tested the 72-hour recovery of all seven mission critical systems. Consequently, the effectiveness of the DRP to meet the requirements in the Emergency Preparedness Plan (EPP) cannot be determined. Although ITS successfully conducts a 48-hour test of selected mission critical systems on a semi-annual basis, the recovery of all mission critical systems within 72-hours remains uncertain.

Management will present to the ITS Steering Committee an overview of the current process, the concurrent storage strategy, and issues that need to be addressed to meet the recovery target as specified in Metro's EPP.

Next Step

MAS will perform a follow-up review to determine completion of this issue.

Attachment: ITS DRP Audit Report

MANAGEMENT AUDIT SERVICES

INFORMATION TECHNOLOGY AUDIT

INFORMATION TECHNOLOGY SERVICES DISASTER RECOVERY PLAN

REPORT NO.
06-ITS-010

JUNE 2006

Metro

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Introduction

Management Audit Services (MAS) conducted an audit of the Los Angeles County Metropolitan Transportation Authority (LACMTA) Information Technology Services (ITS) Emergency Response/Information Technology Recovery Plan (DRP). A DRP defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The DRP provides a systematic process to easily and quickly respond to and recover mission critical systems from devastating events.

This audit was included in MAS' annual plan for fiscal year 2006.

Objective

The objective of the audit was to verify whether the ITS DRP is current, adequate, and effective to ensure the continuity of operations.

Audit Conclusion

ITS DRP is current and adequate, however, the DRP effectiveness cannot be ascertained until ITS executes the recovery of all mission critical systems in a single test.

Summary of Significant Issue

72-Hour Recovery Goal for All Mission Critical Systems Disaster Never Tested

ITS has not tested the 72-hour recovery of all seven ITS mission critical systems. Consequently, the effectiveness of the DRP to meet the Emergency Preparedness Plan's (EPP) requirements cannot be determined. Although ITS successfully conducts a 48-hour test of selected mission critical systems on a semi-annual basis, the recovery of all mission critical systems within 72-hours remains uncertain. We recommend that the Chief Information Officer (CIO) develop, for ITS Steering Committee review, a cost/benefit analysis identifying the costs of conducting a 72-hour test and the risks associated with not completing a full 72-hours test in order to confirm ITS' ability to recover within the DRP and EPP specified timeframe. Management concurred with this finding and will present to the IT Steering Committee an overview of the current process, the concurrent storage strategy, and the issues to be addressed to meet the recovery target as specified in Metro's Emergency Preparedness Plan.

INTRODUCTION

Background

The DRP was developed to restore data processing services in the event of a disruption. The objective of the DRP is to identify and document mission critical processes and procedures to easily and quickly respond and recover from emergency and/or disaster impacts. The goal is to restore mission critical computer operations within 72 hours. The CIO is responsible for maintaining, updating and testing the DRP.

The DRP identifies the following systems as mission critical systems: (1) Financial Information System (FIS); (2) Human Resources Management System; (3) Maintenance & Materiel Management System (M3); (4) Payroll; (5) Revenue Collection/ Universal Fare System; (6) Transit Operations & Trends System (TOTS); and (7) Safety Tracking and Reporting. ITS conducts tests of these mission critical systems on a semi-annual basis to determine whether the DRP is effective.

The DRP was tested on July 2005 at an offsite facility. The primary objective of this exercise was to reconstruct critical systems and applications including FIS and TOTS using back-up tapes stored offsite. The secondary objectives were to recover email servers, Intel servers and the M3 system. Pre-exercise meetings were held with the intent to familiarize recovery support and user teams with their roles in this exercise and their responsibilities within the ITS Emergency Notification & Mobilization Plan and the DRP. Post-meetings were conducted to identify lessons learned. User departments participated to verify and test the integrity of the systems and data.

Scope

The audit scope reviewed the ITS DRP and the scheduled testing conducted on July 2005. The audit did not include the Supervisory Control and Data Acquisition (SCADA) DRP, Advanced Transportation Management System (ATMS) DRP and the EPP.

The audit was conducted in accordance with generally accepted government auditing standards and the Information Systems Audit and Control Foundation's Control Objectives for Information and related Technology (COBIT) and included such tests and procedures as were considered necessary under the circumstances.

INTRODUCTION

Methodology

Our methodology included:

- Interviewing key personnel;
- Reviewing the proposed ITS DRP dated January 10, 2005;
- Attending the post DRP test meeting held on October 19, 2005;
- Reviewing the DRP test analysis document;
- Visiting the offsite backup facility, Iron Mountain; and
- Performing a floor check of the 2nd floor computer room, located at the Gateway Building.

AUDIT RESULTS

Finding #1: 72-Hour Recovery Goal for All Mission Critical Systems Disaster Never Tested

The ITS DRP and EPP state that the objective for computer operations is to restore mission critical systems within 72-hours. There is no basis identified in either the DRP or the EPP explaining the need to have all seven mission critical systems operational with a 72-hour period.

We noted that ITS has not performed a test to recover all seven mission critical systems to validate the ITS DRP and EPP goal. Instead, ITS conducts two semi-annual tests of 48 continuous hours on selected mission critical systems. However, these tests do not confirm ITS ability to restore all listed systems within 72 hours. Therefore, the recovery of all mission critical systems is uncertain during an emergency. Untimely recovery of these systems may result in operational delay and disruption.

According to ITS, performing a continuous 72-hour testing of all mission critical systems requires extensive use of personnel and could leave the agency with insufficient support for the test duration.

To determine transit agency best practice, MAS surveyed five transit agencies questioning whether recovery of all mission critical systems is performed in a single test. Two of five agencies responded. One agency stated that only one system is tested on an annual basis because they only have one mission critical system. The other agency performs testing on an annual basis only on one or two of the five mission critical systems.

Based on this survey, we conclude that LACMTA's DRP testing is more comprehensive than the survey respondents. However, our ability to recover all mission critical systems within 72-hours as specified in the DRP and EPP goal has not been corroborated by testing and remains uncertain.

Recommendation
MAS recommends that the CIO develop, for ITS Steering Committee review, a cost/benefit analysis identifying the resources needed to conduct a test of all seven mission critical systems versus the risk of not conducting such a test within the timeframe specified by the DRP and EPP. The cost/benefit analysis should include an evaluation whether all seven mission critical systems need to be recovered within 72-hours.

AUDIT RESULTS

Management Response

To ensure Metro's ability to recover its mission critical systems within 72 hours following a disaster, ITS is pursuing approval for capital funding to establish a concurrent storage strategy that will significantly minimize the amount of time required to restore Metro's growing volume of data. Currently, ITS manages 30 terabytes of data, or 30,000 gigabytes.

As recommended, the Chief Information Officer will present at the next IT Steering Committee meeting an overview of the current process, the concurrent storage strategy, and the issues to be addressed to meet the recovery target as specified in the EPP.

Finding #2: No Target Dates for DRP Updates

According to COBIT, management should establish change control procedures to ensure that the plan reflects actual business requirements. Critical data and operations should be identified, documented, prioritized and approved by the business process owners, in cooperation with ITS management.

The update process does not have target dates for completion and finalizing the DRP. During our audit, the DRP in effect was dated November 2002 and a revised DRP was drafted in January 2005. In December 2005, ITS management completed the DRP and it was finalized and approved in February 2006. The absence of a current DRP creates confusion among the recovery teams consequently impacting LACMTA's ability to recover mission critical systems.

MAS discussed this issue with ITS management and we recommended ITS include a target date for the review and approval of the DRP in each year's plan. ITS management implemented a process in the Work Activity Calendar to review the ITS DRP annually, each December.

AUDIT RESULTS

Finding #3: Original Draft DRP Needed Improvement

Our review of the January 10, 2005 draft DRP indicated that: a) the listing of mission critical system was not current; b) mission critical systems were not prioritized in the order that they are to be restored; c) personnel contact list, persons authorized to declare a disaster and recovery team organization chart, were not current; and d) transportation arrangements for recovery team members to the hot-site was not addressed.

According to COBIT, management should provide for change control procedures to ensure that the plan reflects actual business requirements. Critical data and operations should be identified, documented, prioritized and approved by the business process owners, in cooperation with IT management.

During the audit, MAS discussed these issues with ITS management and the associated recommendations were addressed and included in the DRP during the audit period. ITS management updated and completed the ITS DRP in December 2005 and it was approved and finalized in February 2006.

We wish to acknowledge the assistance received from the ITS staff. The information and time they provided to us contributed significantly to the overall effectiveness of the audit.

Thu Jun 01 14:24:55 2006

Ruthe Holden
Managing Director
November 2005

Audit Team:
Lizzette Espinoza
Rose Sanchez
Beni Warshawsky

APPENDICES

APPENDIX A

Metropolitan Transportation Authority

Metro Interoffice Memo

Date	May 24, 2006
To	Ruthe Holden Managing Director
From	Elizabeth Bennett Chief Information Officer
Subject	Information Technology Services Disaster Recovery Plan Draft Audit Report No. 06-ITS-010

To ensure Metro's ability to recover its mission critical systems within 72 hours following a disaster, ITS is pursuing approval for capital funding to establish a concurrent storage strategy that will significantly minimize the amount of time required to restore Metro's growing volume of data. Currently, ITS manages 30 terabytes of data, or 30,000 gigabytes.

As recommended, the Chief Information Officer will present at the next IT Steering Committee meeting an overview of the current process, the concurrent storage strategy, and the issues to be addressed to meet the recovery target as specified in Metro's Emergency Preparedness Plan (EPP).

If you have any questions, please call me at ext. 24522.

cc: Lonnie Mitchell

APPENDIX B

LISTING OF ACRONYMS AND GLOSSARY

Acronym	Term	Definition
BCP	Business Continuity Plan	An all-encompassing, "umbrella" term covering both disaster recovery planning and business resumption planning. Also see disaster recovery planning and business resumption planning.
COBIT	Control Objectives for Information and related Technology	Audit standards set by Information Systems Audit and Control Association. These standards represent a consensus of experts to optimize IT-enabled investments, ensure service delivery and provide a measure to evaluate MTA practices against objective criteria.
DRP	Disaster Recovery Plan	The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the started disaster recovery goals.
FIS	Financial Information System	Oracle system that manages LACMTA's finances including vendor payment and procurement.
GAGAS	Generally Accepted Government Audit Standards	Audit standards issued by the Government Accountability Office in 2003 that are used by MAS for all audits and reviews.
	Hot-site	An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Similar Terms: Backup site; Recovery site; Recovery Center; or Alternate processing site.
ITS	Information Technology Services	LACMTA department
LACMTA	Los Angeles County Metropolitan Transportation Authority	
MAS	Management Audit Services	LACMTA department
M3	Maintenance & Materiel Management System	System implemented in 2005 to track and manage inventory and track vehicle maintenance.
O/S	Operating System	O/S makes sure that different programs and users running at the same time do not interfere with each other. It is also responsible for security and handles input/output to and from attached hardware devices, such as hard disks, printers, and dial-up ports.

APPENDIX B

LISTING OF ACRONYMS AND GLOSSARY

TOTS	Transit Operations & Trends System	System that tracks bus operator's hours.
Windows XP	Windows experience	An operating system for Microsoft Windows.