

**DISASTER RECOVERY AUDIT
AUDIT ITS 05-02
FEBRUARY 21, 2006**



CITY OF TAMPA

Pam Iorio, Mayor

Internal Audit Department

Wayne Boytim, Acting Internal Audit Director

February 21, 2006

Honorable Pam Iorio
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

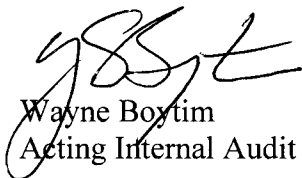
RE: Disaster Recovery Audit, Audit ITS 05-02

Dear Mayor Iorio:

Attached is the Internal Audit Department's report on Disaster Recovery.

We thank the management and staff of ITS for their cooperation and assistance during this audit.

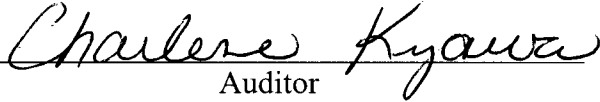
Sincerely,



Wayne Boytim
Acting Internal Audit Director

cc: Darrell Smith, Chief of Staff
John McGrath, Chief Information Technology Officer

**DISASTER RECOVERY AUDIT
AUDIT ITS 05-02
FEBRUARY 21, 2006**


Auditor


Acting Audit Director

DISASTER RECOVERY AUDIT AUDIT ITS 05-02

INTRODUCTION

It is the policy of the City of Tampa Strategic Planning and Technology Services Department to develop and maintain documentation known as the "Disaster Recovery Plan" which will provide every opportunity to withstand a catastrophic event, be it accidental, man-made or natural, and resume essential data processing operations in a swift, efficient and effective manner. It is expected that, with this plan in place, management will be able to provide the swift and decisive leadership that will be necessary for successful recovery. Additionally, because of the guidance provided by the plan, it is expected that the Information Technology Staff will be able to efficiently and effectively carry out their tasks and responsibilities.

The Plan is designed to reduce the risks against operating successfully in the face of various crisis situations and is applicable regardless of when a catastrophic event might occur. It is understood that the probability of a severe disaster is low; however, the plan is considered vital should such an emergency occur.

The ultimate goal of the plan is to resume critical data processing to support the business units within a 12 to 48 hour time frame based upon Continuity of Operations Plan (COOP) business recovery prioritization.

STATEMENT OF OBJECTIVES

This audit was conducted in accordance with the Internal Audit Department's FY05 Audit Agenda. The objectives of this audit were to determine that:

1. The disaster recovery plan was up-to-date and distributed to all Disaster Recovery team members;
2. There were defined locations where the disaster recovery plan could be executed; and
3. The disaster recovery plan was periodically tested and any necessary adjustments were incorporated into the plan.

STATEMENT OF SCOPE

The scope of the audit was limited to ITS and their ability to perform data restoration and not an assessment of enterprise wide Continuity of Operations (COOP) plans. The audit testing emphasized the current status of the material for the period July 2005 through December 2005 rather than historical issues.

STATEMENT OF METHODOLOGY

Source documentation was obtained from Information Technology Services (ITS). Original records as well as copies were used as evidence and verified through physical examination. Computer processed data was not used to arrive at our conclusions; therefore, we are not required to assess or attest to the reliability of this type of data.

STATEMENT OF AUDITING STANDARDS

We conducted our audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to afford a reasonable basis for our judgments and conclusions regarding the organization, program, activity or function under audit. An audit also includes assessments of applicable internal controls and compliance with requirements of laws and regulations when necessary to satisfy the audit objectives. We believe that our audit provides a reasonable basis for our conclusions.

AUDIT CONCLUSIONS

Based upon the test work performed and the audit findings noted below, we conclude that:

1. The responsibility of administrating and coordinating the Disaster Recovery (DR) plan has been assigned to an appropriate individual. The plan was up-to-date and distributed to all the appropriate DR team members;
2. Defined locations have been established where the disaster recovery plan can be executed; and
3. Comprehensive data restoration testing was not performed on a regular basis. Parts of the disaster plan have been tested; however, a comprehensive data restoration test has not been performed since the City entered into an agreement with SunGard for continuity services in October 2003.

While the finding discussed below may not significantly impair disaster recovery functions for the City, they do present risks that can be more effectively controlled.

NOTEWORTHY ACCOMPLISHMENTS

The current Disaster Recovery plan has improved significantly in comparison with the previous plan. Procedures have been put into place to ensure that the plan is kept up-to-date.

Two disaster recovery projects were successfully accomplished since the 2004 hurricane season:

- 1) Acquisition and testing of Tier 0 Emergency Management ITS Equipment. The required ITS equipment was installed and tested at the Emergency Operations Center to support Tier 0 ITS Services. These services represent the base networking and replicated services such as email, the City Internet site, security servers and firewalls.
- 2) Execution of Payroll's Emergency Plan was conducted. On September 27, 2005, a full payroll cycle was executed from the Emergency Operations Center (EOC). This test was deemed to be successful and included the ACH interface to State of Florida for child/spousal support payments and the activation of the ProCheck Disaster Master remote check print/delivery service.

TESTING OF THE DISASTER RECOVERY PLAN

It is essential to test disaster recovery plans to determine whether they will function as intended in an emergency situation. Testing enables plan deficiencies to be identified and addressed and also helps evaluate the ability of the recovery team to implement the plan quickly and effectively. While ITS routinely rebuilds servers as part of their day to day maintenance and have established hot sites for key servers, testing of the overall disaster recovery plan is limited. Although ITS has successfully tested the base network services and executed an emergency payroll test at the Emergency Operations Center (EOC), recovery of most of the City's computer applications and systems have not been tested. The City has entered into an agreement with the business continuity vendor SunGard in October 2003 to provide business continuity services for the mainframe applications at one of their locations. The agreement includes two pre-paid tests per year; however, tests have not been conducted at SunGard since the inception of the agreement.

RECOMMENDATION

ITS should establish a formal schedule for testing comprehensive data restoration. Per the control practices within CobiT¹, disaster recovery tests should be scheduled and conducted on a regular basis or upon major changes to the business or IT infrastructure. The results of each test should be documented and clearly indicate if the test was successful or not. Lessons learned from the test results should be documented and the disaster recovery plan updated as needed. Any weaknesses identified in the testing should be re-tested in the next testing exercise.

AUDITEE RESPONSE

ITS Operations has requested an April 2006 test with SunGard to test recovering the City mainframe. The City agreement with SunGard allows for two test periods per year but both are required to be run concurrent in an additive scheme in order to have enough contiguous hours to fully restore and then test functionality. Though, the actual recovery procedures for the mainframe have remained consistent since the last successful test, each year ITS routinely reviews the environment with SunGard to ensure changes to the environment have been accommodated in the event resource allocation or scheduling prohibit the actual performance of a test. For 2006 and ongoing, ITS will continue to perform a single annual test every April recording the results and lessons learned. Observed weaknesses and lessons learned will go into improving the plan for each successive test. ITS will also continue to investigate alternatives to offsite subscription services for these tests and when feasible propose and implement improved and more effective plans for protecting this critical environment.

¹ COBIT is an IT governance framework and supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout organizations.