



Fairfax County Internal Audit Office

Department of Information Technology
Data Center Disaster Recovery Audit Report
Final Report

September 2006

"promoting efficient & effective local government"

Executive Summary

Our audit found that a comprehensive Fairfax County disaster recovery plan for the data center was in the process of development. Many fundamental components had been addressed; however additional work was needed in the following areas:

Department of Information Technology Responsibilities

- The county disaster recovery plan does not include all non-mainframe computer applications.
- The business impact analysis was incomplete
- Goals and objectives for disaster recovery testing were not defined

Facilities Management Department Responsibilities

- The wet-pipe fire suppression system posed a risk in the data center
- Access to the data center was not well controlled
- Emergency power for the data center was not adequate

An effective disaster recovery plan includes a combination of preventive, detective, and corrective measures to ensure a smooth continuity of business operations in the event of a disruption or disaster. The plan should address the basic stages of emergency reaction: emergency response, backup operations, and recovery operations. Integration with the county's continuity of operations planning (COOP) project should bring more structure and greater coordination to the technology disaster recovery effort.

The county's use of a commercial data center backup has some limitations that present concerns for certain disaster scenarios, especially those associated with regional events. It is possible that the county would not be able to use the backup arrangements if other organizations declare a disaster first or rank more highly in regional or national importance. We support the Department of Information Technology's (DIT) efforts to strengthen the county's internal disaster recovery capacity by building in additional capabilities where possible.

Scope and Objectives

This audit was performed as part of our FY 2006 annual audit plan, because recovery of data and systems is critical for continued county operations in the event of a disaster. This audit was conducted in accordance with generally accepted government auditing standards and covered the period from July 2004 to December 2005. Our objectives were to:

- Determine that a business impact analysis has been prepared to evaluate the loss of critical business processes.
- Determine that systems and other resources required to support critical business processes have been identified and prioritized in the event of a disruption.

- Verify that a detailed plan for the recovery of information system facilities has been established through the development and testing of strategies for recovering critical business processes until full operations are restored.
- Determine that the plan is maintained and updated as the organization changes and new systems and applications are developed and implemented.

Methodology

Our audit approach included a review and evaluation of disaster recovery planning and test documentation, contracts with vendors for the provisions of alternate facilities and application data backup storage. We reviewed records pertaining to the prioritization of applications, inventory records and data center access reports and controls. We interviewed key personnel and used internal control questionnaires to evaluate the pre-planned framework for initiating recovery operations immediately following a disruption or a disaster.

We did not verify the contents of the data center's data backup library. We did not review the contingency plans for the purpose of supporting the continuity of departments' critical service areas.

The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the county executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the county executive and the Board of Supervisors, and reports are available to the public.

Findings, Recommendations, and Management Response

Department of Information Technology Responsibilities

1. Non-mainframe Computer Systems and the Disaster Recovery Plan

The county disaster recovery plan does not include all non-mainframe computer applications. If there is a disaster that affects platforms housed at the data center other than the mainframe, the county would not be totally prepared to handle the disaster or be able to perform recovery in a timely manner for some applications.

The disaster recovery plan (data center) establishes procedures to be followed in the event that data center support is lost for an extended period of time. Procedures are in place to be used by staff for actions to be taken in response to a disaster, recovering computer operations following a disaster, and sustaining essential computer support for the duration of a recovery period. The objective of the plan is to minimize the effects of a disaster upon county operations.

However, losing the capability to process, retrieve, and protect information maintained electronically, regardless of where it resides, can significantly affect a department's ability to accomplish its mission. Examples of applications at risk are: the Harmony System used for case and financial management in Family Services; Tax Administration's new real estate system, the Integrated Assessment System, used for real estate assessed values and tax payment information; and the new retirement system, the Pension Gold Enterprise system, which will administer multiple pension funds. For this reason, an organization should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions, and (2) a plan to recover critical operations should interruptions occur with the data center, the network, and the various platforms (e.g. Unix, client server, etc.).

Recommendation: We recommend that DIT, in concert with data sponsors within agencies/departments, take steps to fully develop and test a plan for the priority non-mainframe systems.

Management Response: DIT has a contract with Sungard Recovery Services, located in Philadelphia, PA. This contract includes mainframe equipment and we are licensed for the use of sixty servers to support non-mainframe applications. DIT has made progress in developing a preliminary plan for supporting non-mainframe applications in a disaster recovery situation. Currently, the MS Exchange (e-mail) system is in a failover mode at the Chantilly Library.

DIT has received \$3 million of funding in 2006 to support disaster recovery. We are currently developing a plan for a disaster recovery infrastructure at the Government Center, Chantilly Library and the Jennings Building.

It will take at least two years with additional funding to have a more comprehensive disaster recovery plan in place to support critical systems. The selection of systems to be supported will be decided through a Senior IT Steering Committee prioritization process. The anticipated completion date is June 2008.

2. Business Impact Analysis Update and Completion

The business impact analysis was not complete. A complete business impact analysis is the foundation for a comprehensive disaster recovery plan, as it determines the priority for the recovery of critical county business applications in the event of disaster. The last effort to develop such an analysis was in September 2003. A complete analysis could not be achieved due to the non-response on the part of about one half of the departments. Further the determination of system recovery priorities had not been finalized as of our audit.

This situation has resulted in an incomplete analysis of applications, and therefore, does not address full recovery in the event of a disruption or a disaster.

A current business impact analysis should fully describe the system requirements, applications, processes and interdependencies to determine contingency requirements and priorities for all applications. These attributes are necessary for the recovery and

timely resumption of critical business operations in the event of a disaster.

Recommendation: The Department of Information Technology should create and maintain a complete and current business impact analysis for recovery planning purposes. This may be accomplished through requiring a periodic update from departments as to existing and recently acquired applications. In order to facilitate obtaining a complete set of responses, the Department of Information Technology should obtain the support from executive management as necessary to mandate the need for departmental compliance.

Management Response: It should be noted that any BIA is a business function requirement as a guide to determining what infrastructure components have to be put in place to support critical county functions. The BIA should be incorporated as part of the Continuity of Operations Plan (COOP) that each agency is required to develop.

We will take actions necessary to gain executive sponsorship and integration with the COOP process, and complete the next BIA with system priorities assigned. The anticipated completion date is March 2007.

3. Disaster Recovery Testing Goals and Objectives

The county has performed a disaster recovery test at the hot site facility maintained under contract with Sungard twice a year. The results of the tests were documented, however, the overall goals and objectives of the testing program were not defined or concluded upon within the documentation, as well as specific input recommendations to assist the development and update for a disaster recovery plan.

According to the National Institute of Standards and Technology Contingency Planning Guide for Information Technology Systems, a test plan should be designed to test selected elements against explicit test objectives and success criteria. The use of test objectives and success criteria enable the effectiveness of each plan element and the overall test plan to be assessed. Test plans should be designed to assess subsets and components of the county's IT services delivery and should enable DIT and departments to evaluate the overall level of disaster recovery readiness.

Even though the results of a disaster recovery test were useful, the lack of performance measures against a set of pre-determined goals and objectives does not provide a full assessment as to the relative success of the individual test plans and the overall test plan strategy.

Recommendation: Future disaster recovery tests should specify goals and objectives of each exercise at the initial test planning meeting. This will enhance the evaluation of the disaster recovery test as well as allow for a meaningful update to a disaster recovery plan.

Management Response: Future test plans will specify goals and objectives of selected elements to show success criteria. The anticipated completion date is October 2006.

4. Unsecured Back Up Media to Off-Site Storage

Data and programs sent to the First Federal Corporation, the county's vendor for the off-site storage for backup, were being placed in unlocked metal containers maintained in the data center. In addition, the backed up data was transported to the off-site location in this manner. The containers provided by the First Federal Corporation, did not have locks to secure the backed up data media.

The use of unlocked containers for the transportation of backed up data pose an increased potential for the loss or theft of data. The potential liability to the county if such an incident were to occur could result in civil damages and regulatory violations depending on the type of missing data.

Recommendation: The Department of Information Technology responded immediately to this situation and backup media are now maintained in locked containers pending and during transport to the off-site facility. The next backup inventory reconciliation with First Federal should require a prompt follow up to any outstanding or questionable items in the data backup inventory schedules to ensure a loss has not occurred.

Management Response: This finding is resolved; all media are stored in locked metal cases. The finding was completed in June 2006.

Facilities Management Department Responsibilities

5. County Employee Access to the Data Center

Access to the data center was not well controlled as we found a large volume of access granted with no apparent business need. Passcard access to the data center for a substantial number of county employees was not linked to job responsibilities or a continuous business need. Over 240 personnel were given access to the data center. There were approximately 174 general county staff not assigned to the Department of Information Technology granted unlimited passcard access without notification or approval from DIT. Of these, 140 employees were assigned to the Facilities Management Department (FMD) with trade maintenance responsibilities. FMD personnel assigned to other facilities possessed unlimited access to the data center. We determined that ten terminated employees were still listed as having access. In addition, many employees from a variety of departments had access to the data center that did not appear to be in line with job duties. The manager of the Enterprise Technology Operations Center did receive a complete data center access report, but it only reported those individuals granted data center access that were working in the Department of Information Technology. This did not provide a sufficient picture of the data center security circumstances.

Access controls are required to reduce the physical exposures to data center equipment, production operations and backed up application data files. This is a preventive measure to safeguard its continuous operation. Authorized access without specific job related justification creates a potential exposure for permitting entry for

other than business related purposes. Access was granted to certain county employees even though the need was temporary or incidental to their main job responsibilities.

Recommendation: We recommend that access to the data center be granted on the least privileged principle. FMD personnel have been removed from the access card entry to the data center and should be required sign in and be escorted to perform any necessary duties. Employees from other departments with present access to the data center should be contacted by FMD to determine the justification for on-going access privileges based on job related necessity. These employees should be removed from access if there is no business justification. Reports provided by FMD to the data center manager from the passcard access system will include all personnel who have access. Access privileges to the data center will include co-approval by DIT.

Management Response: Non-essential employees have been removed from access to the data center. A total of 117 individuals were removed from access to the data center on February 23, 2006. Reports provided by FMD to the data center manager from the passcard access system will include all personnel who have access, not just the DIT personnel. Access privileges to the data center will include co-approval by DIT.

6. Wet Pipe Fire Suppression System in the Data Center

The wet-pipe fire suppression system in the data center posed a potential risk to the county's computer operations. The hardware, current systems, and data backups were subject to water damage.

Wet-pipe fire suppression systems are vulnerable to water leakage and therefore can cause damage to the hardware and stored backup data maintained in the open. Water leakage is a potential hazard that can cause serious damage to computer equipment.

The Department of Information Technology has acknowledged this potential risk as a result of prior audit observations and consultant studies. This issue was previously cited during our prior audit of application data backup.

Recommendation: The existing wet-pipe fire suppression system should be replaced. This will require planning and allocation of funding to reconfigure the fire suppression system. In 2003, it was estimated by external consultants that this would cost approximately \$125,000.

Management Response: DIT has hired a data center consulting firm to perform a comprehensive assessment of the data center. This study will frame the multiple single points of failure (SPOFs) that currently exist in the data center to include: sprinklers, emergency power, cooling system, power distribution, and uninterruptible power. Once this study is complete, a full engineering design will address the shortcomings in the data center as one single project. The comprehensive study is scheduled to be completed in October, 2006. The detailed design is scheduled to be completed in July 2007 and construction is expected to be completed by April 2008.

7. Emergency Power for the Data Center

The un-interruptible power supply (UPS) is a single unit that has a primary generator backup power supply for the government center and a secondary generator backup power supply for the data center. If the primary generator goes down, the building would be supported by the secondary generator intended for the data center, leaving the data center without power.

Emergency power for the data center should be a separate power supply as opposed to being shared with other power sources for the building. The National Institute of Standards and Technology maintains that a system and its data can become corrupt as a result of power failure. A UPS can protect the system if the power is lost and provide enough temporary power to permit a successful shutdown.

There has been awareness within the DIT and FMD as to the vulnerability of this emergency power arrangement through studies and consultants; however, budget priorities and constraints have prevented an immediate resolution to this condition. The present backup arrangement does not provide reasonable assurance the data center could remain in operation in the event of a power emergency.

Recommendation: Alternate emergency power supply arrangements should be studied for the needs of the data center. Optimally, the emergency power source for the data center should be dedicated for that purpose only and have the characteristics of an un-interruptible power supply.

Management Response: As noted in item number 6, DIT has hired a data center consulting firm, to perform a comprehensive assessment of the data center. This study will address emergency power. Once this study is complete, a full engineering design will address the shortcomings in the data center as one single project. Construction is expected to be completed by April 2008.