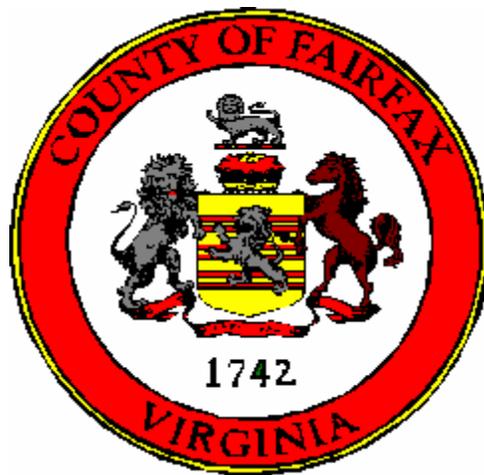


INTERNAL AUDIT REPORT

Audit of Fairfax County Park Authority's Automation Services Branch Back-Up and Recovery Procedures



Fairfax County Internal Audit Office

**FAIRFAX COUNTY, VIRGINIA
INTERNAL AUDIT OFFICE
M E M O R A N D U M**

TO: Anthony H. Griffin
County Executive

DATE: September 17, 2002

FROM: Ronald A. Coen, Director
Internal Audit Office

SUBJECT: Report on the *“Audit of Fairfax County Park Authority’s Automation Services Branch Backup and Recovery Procedures.”*

Attached is the Internal Audit report entitled, *“Audit of Fairfax County Park Authority’s Automation Services Branch Backup and Recovery Procedures”*. It was performed as part of our FY2002 Annual Audit Plan.

The findings and recommendations of this audit were discussed with the Park Authority. We have reached agreement on all of the recommendations and I will follow up periodically until implementation is complete. Their responses are incorporated into the report and the full response is attached at the end of the report. After your review and approval, we will release the report to the Board of Supervisors.

RAC:dh

Attachment

Table of Contents

Introduction	1
Purpose and Scope	1
Methodology	2
Executive Summary	3
Comments and Recommendations	4

Introduction

Fairfax County Park Authority has assigned its data and program backup and recovery function to the Automation Services Branch (ASB). In addition, ASB is responsible for maintaining all hardware, software, telecommunication resources, and supporting Park Authority's centralized systems, including:

- Minicomputers, PCs and thin client terminals
- Management of the network and associated infrastructure equipment
- Systems hardware configuration and maintenance
- Communications configuration for headquarters and 30+ sites
- User software application support
- Help Desk

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. A department should have (1) procedures in place to protect information resources and minimize the risk of interruptions, and (2) a plan to recover critical operations should interruptions occur. These plans should consider the activities performed at general support facilities such as data processing centers and telecommunications facilities, as well as the activities performed by users of specific applications. Recovery plans should be tested periodically in disaster simulation exercises to determine whether they will work as intended.

The Automation Services Branch can provide a high level of assurance that service interruptions will be minimized with adequate controls in place for backup and recovery of Park Authority's data and programs. Periodic reviews, updates and testing of established processes will allow for a quicker response to any interruption that may arise

Purpose and Scope

This audit was performed as part of our FY 2002 long-range audit plan. Our audit objectives were to determine if Park Authority data: (1) Is reasonably and adequately protected from intentional or unintentional damage or loss; and (2) Can be reconstructed or recovered in the event of a loss.

The scope of our audit included an evaluation of the development, execution and testing of Park Authority's Automation Services Branch data backup and recovery procedures for the following systems:

- ParkNet
- MMS
- IVR
- Internet Program Registration
- Credit Card Processing
- General or common-use servers

Our scope was limited to the Automation Services Branch's roles and responsibilities in providing backup and recovery of Park Authority's data and applications. We examined Park Authority's efforts to implement a business impact analysis and business continuity plan. The audit period covered March through June 2002.

Methodology

We reviewed, analyzed and evaluated the Automation Services Branch's management and internal controls over the backup and recovery functions. Our audit approach included:

- Interviewing appropriate employees to obtain an understanding of processes in place
- Testing the ability of off-site facilities' capability to dial-in and continue providing service when connections to the County network have been lost
- Observing a recovery of application data from backup media
- Evaluating the configuration of backup/recovery software and automated processes
- Determining if environmental controls within the operations center are adequately maintained

The audit was performed in accordance with generally accepted government auditing standards. We also used information systems auditing standards due to the technical nature of the audit. These standards include:

- General Accounting Office's *Federal Information System Controls Audit Manual* (FISCAM)
- Information System and Control Association's *Control Objectives for Information and Related Technology* (COBIT)
- Department of Information Technology Policies and Procedures, Memorandum No. 1, *Information Protection Manual*
- Various National Institute of Standards and Technology (NIST) publications and bulletins

Executive Summary

In our opinion, the Automation Services Branch has appropriate procedures in place to manage the majority of its backup and recovery processes. However, lack of compliance with business continuity measures contained within the Department of Information Technology's (DIT) Information Protection Manual could contribute to potential financial and operational harm to the Park Authority if Automation Services Branch was unable to recover operational data, applications, or systems.

Park Authority data is protected from intentional or unintentional damage or loss by daily backup of data and applications, environmental controls in the operations center, including uninterruptible power supply, and physical control over access to the operations center. Park Authority data can be reconstructed or recovered in the event of a loss. Daily backups provide 28 days of recoverable ParkNet data and 20 days of recoverable data from Park Authority file servers. Park Authority successfully tested for recovery of their backup data and validated the appropriateness of procedures in place. The Automated Services Branch will address the need to implement an off-site rotation of all backups at another location. This measure will help to reduce potential loss of data and software programs in the event of destruction of the operations center.

The following section details the areas where Park Authority and Automation Services Branch management can make improvements to help ensure that their operations can be sustained during service interruptions.

Comments and Recommendations

1.1 Automation Services Branch does not keep backed-up media and copies of system-related documentation at an off-site storage facility as required in the Information Protection Manual.

ASB maintains 28 days of backed-up media for ParkNet and 20 days for associated file servers. All backed-up media is maintained within the operations center.

DIT's Information Protection Manual states that, "Agency/department heads are responsible for ensuring that information deemed critical is backed up and stored in a secure location away from the primary usage site." Destruction of the ASB's computer center would render computer operations unrecoverable because all data would be lost.

Recommendation 1.1

Priority: HIGH

We recommend that Park Authority management work with DIT to develop and implement an off-site tape rotation plan and retain off-site copies of system-related documentation. This will enhance Automation Services Branch's ability to recover programs and data in a timely manner following service interruptions.

Department Response

Park Authority has contacted DIT and begun the development of a process and procedure where tapes will be sent on a weekly basis to the Massey Building and returned to Park Authority headquarters on a rotating schedule.

1.2 Park Authority has not documented a business impact analysis as required in the Information Protection Manual.

Park Authority has not determined the operational impact of lost information resources, which is the first step of a business continuity plan.

The DIT Information Protection Manual states that "Agency/department heads will conduct a business impact analysis annually. This process identifies the information created or used within the agency and the consequences to the County's business process if the information were altered or destroyed, or if the method used to process the information was not available."

A business impact analysis provides the basis for setting priorities and action plans in the event of a service interruption. An effective business continuity plan cannot be developed without this evaluation of the operational impact from system outages.

Recommendation 1.2

Priority: MEDIUM

Park Authority management should establish a team of representatives from each operational unit to develop an initial business impact analysis based on the items contained in the Information Protection Manual.

ASB management should conduct an analysis of the operations center as part of this process because it is the core of Park Authority's information system resources and would be most affected by any service interruption.

Department Response

Park authority will establish a team to develop an initial business impact analysis consistent with the requirements described in the Information Protection Manual.

Part of the document will include an analysis of the role of the operations center as the repository of the Park Authority's automated information systems.

1.3 Park Authority has not developed a business continuity plan as required in the Information Protection Manual.

Park Authority has not determined how they would maintain their operations if the computer center were inaccessible or temporarily out of service.

The DIT Information Protection Manual states that "Agency/department heads will maintain a business continuity plan, which allows critical business functions to continue in the event that primary business facilities or resources are not available."

The effect of not developing a business continuity plan is that the management of potential service interruptions would be performed in an ad hoc manner.

Recommendation 1.3

Priority: MEDIUM

We recommend that Park Authority develop and document a comprehensive business continuity plan based on the items contained within the Information Protection Manual.

Department Response

The Park Authority will develop and document a comprehensive business continuity plan based on the items contained within the Information Protection Manual.

2. Automation Services Branch has developed and tested its procedures for the recovery of Park Authority's data and applications.

During the survey phase, it was determined that no documented procedures were in place for the recovery of Park Authority's programs and data.

NIST recently issued a bulletin, *Techniques for System and Data Recovery*, which addresses the need for a formalized testing program. Specifically, "For all procedures used to address organization policy for system and data recovery, it is essential that a test plan be developed and executed at least annually to ensure that recovery is achievable under the prescribed scenarios. Based on the test results, the plan should be modified if required."

ASB documented its procedures for the recovery of data for both its network servers and ParkNet during the early stages of this audit. Testing of the recovery procedures was completed during our audit fieldwork phase.

As a result, Park Authority can rely on ASB's ability to recover files that may be accidentally or inappropriately deleted. However, implementing an off-site tape rotation policy, per recommendation 1.1, will provide Park Authority the ability to recover deleted files from an off-site location.

Recommendation 2

Priority: MEDIUM

ASB should periodically test its ability to fully recover Park Authority's critical systems, applications and data. The testing process should be included as part of any business continuity/contingency initiatives put in place by the Park Authority.

Department Response

Beginning January, 2003 ASB will semi-annually test the branch's ability to recover data from both the Park Authority's file server and the ParkNet application to help ensure that staff are familiar with the process and that critical data can be recovered in the event of a loss of data.

3. Operations center personnel have not been trained in emergency response procedures.

Park Authority has developed a draft version of its emergency response plan. However, the plan does not address the handling of emergencies that may occur within the operations center.

According to FISCAM, "Staff should be trained in and aware of their responsibilities in preventing, mitigating and responding to emergency situations. For example, data center staff should receive periodic training in emergency fire, water, and alarm incident procedures..."

There has been no perceived need to develop and/or provide training in emergency response procedures because FMD personnel are available on-site and responsible for monitoring the environmental controls within the operations center.

In the absence of ASB emergency procedures, the Park Authority emergency response plan will be incomplete. ASB would need to completely rely on FMD personnel to assess and manage potential operations center emergency situations.

Recommendation 3

Priority: MEDIUM

We recommend that ASB actively participate in development of sections within the existing draft emergency action procedures that relate to the computer operations center.

Also, a training program should be developed to ensure that personnel working in the operations center could properly operate emergency equipment as required. Refresher training should be completed annually to maintain proficiency in the use of such equipment.

Department Response

The ASB manager is participating in the development and review of the Herrity Building's Emergency Response Plan (ERP).

Using the content of the Emergency Response Plan as a guide, the ASB manager is developing a brief seminar which describes and identifies the electrical, mechanical, fire suppression, and alert systems in the operations center. This brief seminar will be given to all ASB staff and shared with the Department of Planning and Zoning, which also occupies the operations center.

Refresher training will be given on an annual basis each November.