SOUTH FLORIDA WATER MANAGEMENT DISTRICT

AUDIT OF FINANCIAL SYSTEM'S CHANGE CONTROLS AND BACKUP/RECOVERY PROCESS CONTROLS

Audit 01-21

Prepared by
Office of Inspector General

Allen Vann, Inspector General
John Lynch, Lead Information Systems Auditor
Tim Beirnes, Lead Consulting Auditor

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

3301 Gun Club Road, West Palm Beach, Florida 33406 • (561) 686-8800 • FL WATS 1-800-432-2045 • TDD (561) 697-2574
Mailing Address: P.O. Box 24680, West Palm Beach, FL 33416-4680 • www.sfwmd.gov

MGT 08-06F
December 4, 2001

Audit Committee Members:
Mr. Gerardo B. Fernandez, Chair
Mr. Lennart E. Lindahl, Vice-Chair
Ms. Pamela D. Brooks-Thomas, Member
Mr. Michael Collins, Member
Mr. Patrick J. Gleason, Member

Re: Final Report – Audit of
Financial System's Change
Controls and Backup/Recovery
Process Controls, Audit # 01-21

This audit was performed pursuant to the Inspector General's authority set forth in Chapter 20.055, F.S. The audit focused on an incident involving program change controls and the backup/recovery process for the District's financial application program and the supporting computer operating system. Mr. John T. Lynch, Lead Information Systems Auditor and Mr. Tim Beirnes, Lead Consulting Auditor prepared this report.

Sincerely,

Allen Vann
Inspector General

AV/jl
Enclosure

c: Henry Dean
John Fumero

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

TABLE OF CONTENTS

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

INTRODUCTION

This audit was performed pursuant to a request from the Director of Information Technology. On August 14, 2001 the Director of Infrastructure Services informed the Inspector General's Office of an incident that seriously impacted the operations of the computer system that contains the District's financial data. The incident occurred on July 27, 2001, resulting in an interruption that lasted for three days. This incident(s) involved the corruption of the general ledger file within the computer system and, later, the inability of the staff to recover the file from the normal backup copy. As a result, the general ledger had to be "rebuilt" over the weekend of July 28th.

Based upon information provided to us, we agreed that an audit of the "change control" procedures for the District's financial application system and supporting computer operating system was necessary.

BACKGROUND

The South Florida Water Management District (the District) maintains two minicomputers for database applications and the finance/human resources business functions. These systems are the Alpha 4100 and the VAX 6620 respectively and are also referred to as DEC systems. These computers both utilize an operating system known as Open VMS.

Both computer systems and their supporting peripheral devices are located in the main computer room on the third floor of the new Emergency Operation Center building at the District main campus. The computer room has one full-time first shift computer operator and a part-time operator to support second shift data backup activities.

The District's *Oracle* Database programmers support the database applications for the Alpha 4100. The LGFS Financial and Ross Human Resources/Payroll programming staff supports the application programs for the VAX 6620. Additional system level support for these two computers is provided by the District's "Oracle system administrator" and contracted "VMS system administrators."

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this audit were to determine the root cause for both the loss from within the District’s financial computer system of the general ledger data file and the inability of staff to recover the file from the “nightly cycle” data backup by:

- Ascertaining whether staff (including contractor staff) was following generally accepted practices for computer operations and application program support.

- Ensuring that there were sufficient controls in place to protect the District financial computer’s operating system, application programs and data files.

The scope of this audit covered the procedures used to support the District’s financial and Human Resource/Payroll applications running on the VAX 6620 computer, its operating system, and the associated backup and recovery process.

The methodology included:

1. Reviewing current VAX 6620 computer operation and operating system support process.

2. Evaluating the Information Systems controls over:

    - Security and Access to the systems,
    - Backup & Recovery of data files, and
    - Program, Data and Operating System changes.

3. Interviewing applications support staff, operations/system support staff, contracted operations/systems support staff, and supervisory staff.

This audit was conducted in accordance with "generally accepted government auditing standards" as promulgated by the Comptroller General of the United States. In addition, we were guided by the "Standards for Information Systems Auditing" as developed by The Information Systems Audit and Control Foundation Standards Board. Fieldwork for this audit was concluded in October 2001.

EXECUTIVE SUMMARY

We found that the incident resulted from compounded departures from acceptable Information Systems operating practices. First, an inadequately tested change corrupted the general ledger file and secondly, an unauthorized change to the computer's Open VMS operating system corrupted the backup files.

We found that physical access controls were good and did not contribute to the incident. However, there was no formal process in place to control access to the Operator and System Administrator account passwords. Conflicting duties of Operator and System Administrator, which should have been separated, were assigned to a Contractor hired to support computer operations. Furthermore, there was no documentation or review of the daily activities of the Contractor and change control procedures for the financial applications were not followed. Finally, the verification feature that would have detected errors during the creation of the financial backup files (save sets) was not used.

We recommend that:

- A formal procedure be adopted for assignment of access to the operator and system administrator accounts,
- Separation of duties for support staff,
- System administrator and technical support staff activities should be documented and reviewed by supervisory staff,
- Staff should review and enforce change control procedures, and
- A "verify" function should be used during the creation of the nightly cycle backups.

We commend the Director of the Infrastructure Services Division for initiating a formalized comprehensive process for "change control" including procedures, guidelines, and policy. Following this process will contribute significantly to resolving control deficiencies, which could result in a recurrence.

FINDINGS and RECOMMENDATIONS:

In order to determine the root cause for the corruption of the District’s financial systems general ledger file and the inability of staff to recover the file from the “save set” backup, we reviewed the controls over the physical access to the computer room, logical (password) access computer operating system, operating system change controls, and the application system change controls.

Physical Access to the Computer System

Access requests for the District’s main computer room go to the Director of Infrastructure Services. The Director sends an authorizing e-mail to the Security Office. Periodic Security Office reports of individuals who have access to the computer room are sent to the Director of Infrastructure Services for review.

With the use of electronic security cards, only authorized staff have physical access to the District’s main computer room. “A locked room is still considered the best security.”[1] We found that physical access is adequately controlled and did not contribute to this incident.

Logical Access to the Computer Operating System

The computer operators and the System Administrator for the VAX 6620 use two special system accounts. One account is called “operator” and is used to control day-to-day computer operation activities. The other account, called “system,” is used for system administrative functions. Each of these accounts is protected by its’ own password. In the Information Systems Security Audit performed by our office in 1998 we stated that, “there is no formal approval process for the establishment of system administrator privileges.”[2] We could find no formal authorizing process for providing or removing password access to support staff. However, the passwords are routinely changed every ninety days.

[1] Sutton, L. L. & Caniglia, D. F. (2001), *Handbook of IT Auditing*, Boston; Warren, Gorham, & Lamont, E2-6.

[2] *Audit of the District’s Information Systems Security* (Report No. 98-03). South Florida Water Management District, p.15.

Because the District's full-time computer operator was on scheduled off-site technical training and the VAX 6620 system administrator position was vacant; a consultant was hired from TEK Systems for operations and system administration support. The consultant was provided with the passwords to the operator and system administrator account. We could find no documentation authorizing the assignment of passwords to the consultant.

In addition, physical access to the computer room is not required to utilize the password protected operator or system accounts. Any user who has a District network dial-in account and either the operator or the system account passwords can access the system at the operator or system administrator level. This presents an opportunity to bypass physical security.

Recommendation:

1. **Formal procedures should be adopted for granting and revoking access to the operator and the system accounts for both staff and consultants. This should include a review of user access to the dial-in accounts.**

   Management Response: The current operators do not have system manager access. The operators use an operator's account that allows them to perform all the operator duties required. There is only one person at the District who uses the system manager account. All other FTE's or contractors must be approved by the IT employee responsible for overseeing the VAX operations to have access to system manager passwords.

   Auditor's Comment: The inclusion of an approval/removal form with authorizing signatures would formalize the access process and tighten up controls.

   Responsible Department/Office: Information Technology

   Estimated Completion Date: Completed

Operating System Change Control

The District contracted with Compaq Computer Corporation for a DEC Systems (VAX 6620 & Alpha 4100) performance analysis. The components that most affect the system performance (the Central Processing Unit, Memory, and the Input/Output subsystems) were reviewed. In order to evaluate these components the Compaq consultant was given the system password.

Compaq issued a final report on July 17, 2001. The report contained eight (8) specific recommendations for improving the performance of the DEC 6620 system. These eight recommendations included computer “start up” changes, VMS system parameter setting changes, user account authorization changes, and upgrading the DEC 6620 computer to a DEC 6630 or 6640.

District staff indicated that one system parameter setting, page fault, was approved for implementation as recommended in the Compaq report.[3] In order for the recommended page fault change to be in effect the system would require a reboot (restart). This change was to be made prior to the scheduled July 18, 2001 reboot of the VAX 6620. No documentation of this approval was provided.

District staff believes that the page fault parameter change was made by the consultant from TEK Systems. Staff further indicated that the consultant was instructed not to make any unauthorized changes to the VAX 6620 operating system. However, it appears that this same consultant, who was acting as both operator and system administrator, may have made other changes to the parameter settings. The "separation of duties" guidelines for information systems control recommends that computer operators should not have system administrator responsibilities.[4] This lack of separation of duties provided the consultant with the opportunity to make unauthorized changes.

In researching the subsequent incident District staff found that the system audit log file that maintains a history of such changes was either not produced or had been deleted. Staff could not determine when changes were made to the VMS system or who made them. In our review we found no evidence that

[3] There are over 250 parameter performance settings that affect both the VMS operating system and user accounts.

[4] Information Systems Audit & Control Association (2001), *CISA Review Technical Information Manual*. p.85.

any formal change control procedures (with the necessary documentation, testing, and approvals) for the VMS operating system and/or user account settings was followed.

There appeared to be a lack of supervisory attention to establishing and enforcing strong operating system change controls, including a lack of documentation of change authorization and oversight of consultants' work activities. The consultants hired for computer operations and system administration activities only documented “hours worked”. In the Information Systems Security Audit we had recommended that, “a process should be established for documenting the activities of the system administrators.”[5] We could find no documentation of the consultant’s daily activities.

Unauthorized changes to the operating system and user account parameters occurred as a result of inadequate controls and oversight. This lead to an undetected failure in the District’s nightly LGFS cycle file backup “save set” procedure. Consequently, the “save set” files that are normally used to restore the LGFS system were corrupt.

However, the Director of the Infrastructure Services Division has initiated a formalized comprehensive process for “change control” including procedures, guidelines, and policy. This process includes weekly change control meetings, forms for documentation and approval of change requests, service interruption reporting forms, and an IWEB calendar for scheduling changes. (See appendix A.) This procedure applies to IT application, server, database, network and communications systems activities and includes all of the Divisions within the Information Technology Department. The staff meets weekly to review change control requests. This formal process should provide the necessary documentation (audit trail) and authorization approvals that are part of a well-managed systems change control process.[6]

Recommendations:

2. **The staff should maintain separation of duties between the functions of the computer operators and the system administrator (system programmer). This separation of duties should also include the system administrator not having application programming duties.**

[5] *Audit of the District’s Information Systems Security* (Report No. 98-03). South Florida Water Management District, p. 15.

[6] Information Systems Audit & Control Association (2001), *CISA Review Technical Information Manual*. p.301

Management Response: Currently these duties have been assigned to separate staff with clear separate responsibilities. Operators only have access to perform operations for which they are responsible.

Responsible Department/Office: Information Technology

Estimated Completion Date: Completed

3. Systems Administrators and technical support staff (including contracted support) should document their activities, and supervisory review should be evident.

Management Response: All infrastructure changes to production systems within IT must be approved in advance and presented for discussion, evaluation and concurrence by the IT change control group.

Responsible Department/Office: Information Technology

Estimated Completion Date: Completed

Application System Change Control

Because a standard methodology for controlling changes to production application programs is necessary,[7] the application program support staff use a Service Request (SR) form to authorize and document changes to the financial (LGFS) systems (See appendix B). Previously, the SR process was reviewed during the Audit of the District's Information Systems Security and we stated that:

> "Changes to the Financial Systems production programming environment is controlled by the System Integration Division (SID) staff. SID maintains multiple computer operational environments in support of the District's Financial Systems. These include programs/data environments for development, testing, training, and production. Programs are tested and the staff, prior to moving programs or program changes into production, performs a quality assurance review. Written standards exists for "Systems Analysis", "Program Documentation", and a formal "sign-off" process is in place to track changes to program or data files.
>
> These changes are documented with a Service Request Form #770 that is normally initiated by the user and a Service Request Quality Assurance Review Report initiated by the SID staff and approved by a SID supervisor. These forms provide both an audit trail for activities against the production systems as well as authorization signature approvals."[8]

This incident occurred when a Sr. Programming Analysts performed a routine fiscal year-end procedure to split the general ledger file by fiscal year (FY) into two files. The source code used to split the general ledger file between fiscal years reads the current general ledger file, determines which FY the record belongs to and then writes a new record to one of the two respective FY data files. The split general ledger computer program instructs the computer to write records from the current file to one of two new files. The Sr. Programming Analysts inadvertently omitted the "From" command in the

[7] Information Systems Audit & Control Association (2001), *CISA Review Technical Information Manual*. p.301

[8] *Audit of the District's Information Systems Security* (Report No. 98-03). South Florida Water Management District, p. 33-34.

program "Write Statement"; thus the program merely wrote blank records (i.e. all zeros) to the new files.

Adequate testing was not performed in the test environment and the error was not detected until after the changed general ledger file was moved into production and the original file deleted. The service request process "quality assurance review" should have prevented this incident from occurring. However, we could find no documentation for this step (general ledger split) in the year-end process. Established procedures were not followed.

With the general ledger file corrupted, the District's financial system (LGFS) and human resource/payroll (ROSS) systems were not able to function properly. On July 27, 2001 business activities on both systems were interrupted. The staff attempted the normal recovery procedure of restoring the general ledger from the nightly cycle "save set" backup. It was then determined that the daily "save sets" going back to July 18th were corrupt. The staff had to make extraordinary efforts to restore the general ledger file from other system backup files referred to as "incremental" and "full" backups. The file was restored on August 30, 2001. In order to restore the operating system parameter settings, the staff utilized a January 2000 backup copy of the operating system parameters.

Disk-to-disk copies of the LGFS (master) data files, using VMS operating system's standard "save set" backup process, are made prior to updating with the current day's transactions. These backup "save sets" are then copied from disk to magnet tape each morning by the computer operations staff. As stated previously the unauthorized changes made to the VMS operating system and/or the user authorization parameters, resulted in the failure in the "save set" backup process. This failure went undetected from July 18, 2001 until the attempt was made on July 27, 2001 to restore the general ledger file.

During the creation of the "save sets" a "verify" function, which detects error during the file copy process, would have reported these errors. The verify function reads the backup file (copy) and compares it to the source file (master). Any differences are reported as errors. (Using this feature increases backup time by approximately 50% and leads to the temptation to turn off the function in order to save computer time.) Staff does not use the verify function during the process of creating the nightly cycle "save set" backups. In order to ensure the integrity of the "save set" backups, staff should use a verify command option.

Recommendations:

4. **Staff should review and enforce change control procedures to ensure that prior to deleting original programs and/or data files adequate tests have been conducted, test results verified, and authorizing approval given for implementing the change in the production environment.**

   Management Response: Staff will enforce change control procedures as defined in our internal service request procedures and in Information Technology's change control procedures. The steps followed for this particular step in the year end close are documented in a separate procedure/checklist. The entire accounting fiscal year-end close process is outlined, documented and updated each year by accounting with input from IT. Because it is a months long process with over 100 steps, we do not require accounting to process the standard service request for each step.

   Responsible Department/Office: Information Technology

   Estimated Completion Date: Completed

5. **The verify function or an alternative should be used to ensure that backup copy "save set" files are identical to the source (master) files.**

   Management Response: Using the verify option on a daily basis would effectively double the backup and negatively affect the IT staff. The backup system is very reliable and stable unless improper system level changes are made. Management has already implemented a change control process. System changes are only made on weekends and the backup system is tested after each change. Therefore, management will plan to use the verify option only on the weekends when it will check the accuracy of the backup system and not adversely affect the IT staff.

   Responsible Department/Office: Information Technology

   Estimated Completion Date: December 14, 2001

GLOSSARY of TERMS

These definitions were developed by District staff or were drawn from the "Free On-line Dictionary of Computing," by Dennis Howe @ Web Site www.foldoc.org.

AMS *(AMS system, LGFS or Advantage)*

American Management Systems, Inc. is a software development and marketing company located in Fairfax, Virginia. The District utilizes the AMS Local Government and Financial System for financial/administrative management (now referred to as the Advantage System.)

application program *(Or "application")*

A complete, self-contained program that performs a specific function directly for the user. This is in contrast to systems software such as an operating system (OS), which exists to support application programs.

audit trail *(computer)*

A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.

backup

A spare copy of a file or system of files, usually kept on magnetic tape or other removable medium, for use in the event of failure or loss of the original files or system.

change control

In a computer production program or database application, the process of administering modifications to the programs or data. This includes administrative authorization approval and providing an audit trail for modification activities.

DEC

Digital Equipment Corporation. The manufacturer of the District's VAX 6620 and Alpha 4100 computer was purchase by Compaq Computer Corporation.

hardware

The physical, touchable, material parts of a computer or other system. The term is used to distinguish these fixed parts of a system from the more changeable software or data components.

information systems security

Control techniques and measures applied to an Information Technology Process that satisfies the business requirement to safeguard information against unauthorized use, disclosure or modification, damage or loss and is enabled by physical, logical and administrative controls which ensure access to systems, data and programs is restricted to authorized users. (Brian A. Coleman, CISA)

LGFS

See AMS.

operating system (OS)

The low-level software, which scheduled tasks, allocates storage, handles the interface to peripheral hardware and presents a default interface to the user when no application program is running.

password

An arbitrary string of characters chosen by a user or system administrator and used to authenticate the user when he attempts to log on in order to prevent unauthorized access to his account.

platform

Specific computer hardware. It may also refer to a specific combination of hardware and operating system.

recovery

The process of restoring computer data file with a backup copy usually after a crash or accidental deletion of a file.

Ross

Ross Systems, Inc. is a software development and marketing company located in Redwood, California. The District utilizes the Ross Human Resource and Payroll System. Also referred to as the Ross system or HR/PR.

software

Computer programs, as opposed to the computers on which they run (the "hardware").

user(s)

The people who either use computers directly, or use the information they provide; also called computer users or end users.

VMS (Open VMS)

The computer operating system (see “operating system”) for both the DEC VAX 6620 and Alpha 4100 computer systems.

Appendix A

IT Infrastructure Change Management Request Form

Change Title:		**REF #:**	
Change Description:	Overall description of the nature of this change and reasons for implementation. Describe the expected benefits.		

Date Submitted:		**Sponsor:**	Implementation Coordinator Name
Type:	Planned or Emergency Change	**Equipment:**	Name, Type
Risk Level:	Low, Medium or High	**Classification:**	New, Replacement, Upgrade, etc.
Risk Assessment:	Describe risk of change and risk mitigation:		
Impact Level:	Low, Medium or High		
SFWMD Impact:	Describe impact during and after change.		

Implementation Schedule:				
Specify when the change will occur. Attach timeline or Change Management Plan as needed.				
Change Date:	**Install Start Time:**	**Duration:**	**Blackout Start Time:**	**Duration:**

Dependencies:	Note change requirements or special scheduling circumstances. Identify concurrent critical dependencies.

IT Infrastructure Services Group Review:	
Indicate the individuals with whom the Change Request was reviewed.	
DBA Group	Name of Reviewer
Help Desk Group	Name of Reviewer
Network Group	Name of Reviewer
NT Group	Name of Reviewer
Radio/MW Group	Name of Reviewer
UNIX Group	Name of Reviewer
Group Name	Name of Reviewer
Group Name	Name of Reviewer
Group Name	Name of Reviewer

Change Control Team Sign-Off:	
Final approval of Change Management Plan. (Weekly Review Meeting)	
Name	Signature
Name	Signature
Name	Signature
Name	Signature
Name	Signature
Name	Signature
Name	Signature
Name	Signature
Name	Signature

Appendix A (Continued)

IT Infrastructure Change Management Request Form

SFWMD Announcements:
Note communication method and audience. Enter/attach text of notification.
Implementation Plan:
Describe the scope and detailed steps to be performed, or attach Change Management Plan.
Test/Validation Plan:
List test/verification activities to occur before, during and after change implementation.
Back-out/Recovery Plan:
Describe the procedure to reverse the change if necessary.
Contingency/Risk Mitigation Plan:
Describe what can be done to mitigate risks or provide backups/alternatives.

Authorizations:

Name	Signature	Date Approved
Group Supervisor		
Configuration Control Coordinator		
Director or Senior Advisor		
Senior Management Review Team Member		
Architectural Review Group Member		

SOUTH FLORIDA WATER MANAGEMENT DISTRICT

Appendix B

INFORMATION APPLICATIONS (IAD) SERVICE REQUEST

IT SR # **IAD SR #**

THE FOLLOWING INFORMATION MUST BE FILLED OUT PRIOR TO SUBMITTING THE SERVICE REQUEST TO IAD. THE REVERSE SIDE WILL BE FILLED OUT BY THE IAD STAFF.

TO BE FILLED OUT BY THE CUSTOMER
Please attach any additional documentation (e.g., report samples, etc.)

SUBMITTED BY:	**DIV #:**	**DATE NEEDED:***	**REQUESTED PRIORITY:** □1 □ 2 □3 **(1 is the highest)**
	EXT. #		

BRIEF DESCRIPTION / SUMMARY:

DETAIL DESCRIPTION / SERVICE REQUESTED:

REQUESTING DIV. DIRECTOR APPROVAL:	**DATE:**

*** If this is a time sensitive task, obtain Requesting Department Director approval**

REQUESTING DEPARTMENT DIRECTOR APPROVAL:	**DATE:**

REVERSE SIDE IS FOR IAD USE ONLY

Appendix B (Continued)

INFORMATION APPLICATIONS (IAD) SERVICE REQUEST

IT SR #		**IAD SR #**	

THE REVERSE SIDE MUST BE FILLED OUT BY THE CUSTOMER PRIOR
TO SUBMITTING THE SERVICE REQUEST TO IAD

FOR IAD USE ONLY

DATE RECEIVED:						
INITIAL ESTIMATE:	**APPLICATION**	□ **Advantage**	□ **ROSS**	□ **M&P**	□ **OTHER**	
DATE PRIORITIZED:	**TYPE**	□ **Report**	□ **Program**	□ **Maintenance**	□ **Implement**	□ **Other**
PRIORITY ASSIGNED:	**COMPLEXITY**	□ **Simple**	□ **Moderate**	□ **Complex**		

ASSIGNED TO:	**DATE ASSIGNED**:
ESTIMATED MAN-DAYS:	**EST. COMPLETION DATE**:
REQUESTING USER APPROVAL OF EST. COMPLETION DATE (If different from 'date needed' requested on reverse side of form) AND AMOUNT OF TIME REQUIRED TO COMPLETE THE SERVICE REQUEST:	**DATE:**

SERVICE REQUEST / STATUS REPORT

TASK STEP	DATE STARTED	DATE COMPLETED	NOTES
Interviews			
Questionnaires			
Flow Charts			
Input Designs			
Output Designs			
Analysis			
Cost Benefit			
Programming			
Unit Testing			
Documentation			
Customer Testing			

IAD STAFF COMPLETION SIGNOFF

IAD Staff:	**Date:**

CUSTOMER COMPLETION SIGNOFF

Customer:	**Date:**