Memorandum from the Office of the Inspector General

September 20, 2007

John E. Long, Jr., WT 7B-K

REQUEST FOR FINAL ACTION – AUDIT 2007-039T-02 – BACKUP VERIFICATION

Attached is the subject final report for your review and final action. Your written comments, which addressed your management decision and actions planned or taken, have been included in the report. Please notify us when final action is complete.

If you have any questions, please contact Phyllis R. Bryan, Project Manager, at (865) 632-4043 Jill M. Matthews, Director, Information Technology Audits, at (865) 632-4730. We appreciate the courtesy and cooperation received from your staff during the audit.

Ben R. Wagner
Deputy Inspector General
ET 3C-K

PRB:SDB
Attachment
cc (Attachment):
Steven A. Anderson, SP 5A-C
William R. Brandenburg, Jr., MP 2B-C
Frank A. Foster, OCP 2C-NST
Tom D. Kilgore, WT 7B-K
Janice W. McAllister, EB 7A-C
Richard W. Moore, ET 4C-K
Emily J. Reynolds, OCP 1L-NST
E. Wayne Robertson, SP 5A-C
OIG File No. 2007-039T-02

BACKUP VERIFICATION OF TVA PRODUCTION SYSTEMS

Audit 2007-039T-02
September 20, 2007

Synopsis

- In summary, we found:
  - All but 20 production distributed servers, all production databases, and the mainframe were being backed up at the time of our testing. Information Services (IS) provided explanations and/or actions taken for the 20 servers not being backed up.
  - Thirteen obsolete or inactive backup "policies."[1]
  - Nine servers with undocumented exclude lists.
- Based on other observations noted during the audit, we believe an overall process design review could facilitate a better integrated and more efficient backup and restore process.

[1] Policies are rules within the software used to backup servers.

Background

- Backup and Disaster Recovery (DR) requirements are driven by Service Level Agreements (SLA) negotiated between IS and Application Owners. If specific DR requirements are not defined, a standard schedule of a weekly full backup and daily incremental backups is performed on the server.
- Over the past year, TVA has experienced two backup failures (one of which resulted in loss of employee data and the other resulted in loss of transmission system health data) and a “near” miss in November 2006 (backup personnel were reconciling client list and found one client was missing; however, no data loss occurred).
- In February 2007, TVA implemented a verification process to check weekly for additions and removals of servers from the backup system. The new matching process would not identify servers missing prior to February.
- As a result of the PRIS backup failure in March 2007, the OIG was requested to perform a full backup verification of all TVA production systems.

Objective, Scope, and Methodology

Objective

- Verified the necessary backups were being performed on servers and related databases.

Scope and Methodology

- Interviewed IS personnel.
- Obtained server, application, and database information from IS personnel, HP Service Desk, and the DBA monitor Web page.
- Obtained backup reports from IS personnel and the NetBackup Web page.
- Verified servers identified with the role of production in HP Service Desk either (1) were backed up or (2) were known exclusions from being backed up.
- Verified Oracle, SQL Server, and DB2 database backups to disk were also being backed up to tape.

Objective, Scope, and Methodology

Scope and Methodology (cont'd)

- Verified the frequency of backups supported the DR level assigned either to the server or to the applications/databases hosted on the server.
- Reviewed the NetBackup policies for full backups.
- Reviewed the reasonableness of the exclude file listing for each server.
- Fieldwork was conducted between May and August 2007.
- This audit was performed in accordance with generally accepted government auditing standards.

Findings

Distributed Servers

- Of the 1,102 production servers, we determined 1,082 servers were being backed up.
- For the 20 servers which were not being backed up, IS provided the following explanations:
  - Three servers had been retired but still had the role of “Production” in HP Service Desk.
  - Three servers contained no data, thus requiring no backup.
  - Three non-IS supported servers which were functioning as workload balancing servers did not contain any data. According to the Application Owner, no backups were required for these systems.
  - One server was experiencing performance problems which prevented it from being backed up on a regular schedule. IS discontinued backups when the data from an older system was being converted to a storage location for review by the Business Owner. We confirmed the server where this data is stored was being backed up.
  - Ten production servers (one of these is used for program development but still classified as “Production” in HPSD) were identified as having no defined backups. During the course of our audit, IS created work orders to initiate backups for these servers. IS subsequently decided to reassess the backup needs of these servers.

Findings (cont'd)

Mainframe

- We determined the mainframe was receiving scheduled backups.

Databases

- We determined the 379 Oracle, SQL, and DB2 databases were receiving scheduled backups to tape.

Backup Policies

- Policies are rules that the backup software follows when backing up servers. A "full" policy is used to perform a complete backup of the server. We identified 201 full policies across 20 primary backup servers. Of those policies, three were inactive and ten were obsolete. IS plans to remove the obsolete policies.

Exclude Lists

- Exclude lists define files and/or directories that will not be backed up on a server. Our understanding is groups other than the Backup Group (i.e., System Administrators) have the ability to make changes to the exclude list. For nine servers, IS did not have supporting documentation for the exclusions.

Other Observations

- We believe management should consider an overall process design review to develop a better integrated and efficient backup and restore process. The review should address issues previously found in OIG audits, Summary of Aggregated Gap design control deficiencies (such as backup verification, controls implemented as a result of the backup failures), and the following observations:
  - There appears to be a lack of integration/communication between the groups with key responsibilities in the backup process.
  - Multiple Service Levels (4) and DR Classes (4) may be contributing to a more complex environment than necessary.
    - Customers have been able to choose a wide variety of combinations between service levels and DR classes (16 total combinations).
    - IS has not yet synchronized applications and data based on service levels and DR classes (i.e., many database instances have data for applications that have two or more service levels).
  - Server roles were not always accurate in HPSD – three servers classified as production were actually retired.

Recommendations

We recommend the Chief Administrative Officer and Executive Vice President, Administrative Services:

1. Ensure the exclude lists are reviewed for appropriateness. Additionally, a process should be developed to ensure all requests for (a) addition to and/or (b) deletion of files to be backed up are properly documented, reviewed, and approved.
2. Consider initiating a business process review to develop a better integrated and more efficient backup and restore process.

Recommendations (cont'd)

TVA Management's Comments – The Chief Administrative Officer and Executive Vice President, Administrative Services, agreed with our facts, conclusions, and recommendations and provided proposed actions to implement our recommendations. TVA management plans to (1) initiate periodic reviews of the backup schedules and exclude lists; (2) document procedures to maintain the exclude lists; and (3) initiate a process redesign to improve the backup process (see Appendix for entire response).

Auditor's Response – We concur with management's proposed actions.

September 18, 2007

Ben R. Wagner, ET 3C-K

REQUEST FOR COMMENTS - DRAFT AUDIT 2007-039T-02 - PERSONNEL RECORDS IMAGING SYSTEM - BACKUP VERIFICATION

Attached is our response to your August 24 request for comments regarding the findings of the subject report. Also included is information on the Risk Management process results for the findings.

We would also like to thank both Brian Childs and you for the professionalism and cooperation in conducting this audit. If you have any questions, please contact Bill Brandenburg.

John E. Long, Jr.
Chief Administrative Officer and
Executive Vice President
Administrative Services
WT 7B-K

WRB:JSE
Attachment
cc (Attachment):
Steven A. Anderson, SP 5A-C
William R. Brandenburg, Jr., MP 2B-C
Brian S. Childs, ET 3C-K
Frank A. Foster, OCP 2C-NST
Janice W. McAllister, EB 7A-C
Elizabeth C. McBee, WT 5C-K
Charles H. McFall, Jr., MP 2B-C
E. Wayne Robertson, SP 5A-C
EDMS, WT CA-K

Findings	Recommended Action	Risk Management Information	Response

Distributed Servers
 	
• Of the 1,102 production servers, we determined 1,083 were being backed up.
 	
• For the 20 servers which were not being backed up, IS provided the following explanation:
  • Three servers had been retired but still had the role of "Production" in HP Service Desk.
  • Three servers contained no data, thus requiring no backup.
  • Three non-IS supported servers which were functioning as workload balancing servers did not contain any data. According to the Application Owner, no backups were required for these systems.
  • One server was experiencing performance problems which prevented it from being backed up on a regular schedule. IS discontinued backups when the data from an older system was being converted to a storage location for review by the Business Owner. We confirmed the server where this data is stored was being backed up.
  • Ten production servers (one of these is used for program development but still classified as "Production" in HPSD) were identified as having no defined backups for these servers.
	1. Ensure the exclude lists are reviewed for appropriateness. Additionally, a process should be developed to ensure all requests for (a) addition to and/or (b) deletion of files to be backed up are properly documented, reviewed and approved.
	
	2. Consider initiating a business process review to develop a better integrated and more efficient backup and restore process.
		RMF 2007-292
		Potential Impact: Moderate
		Likelihood: Moderate
		Risk Rating: Moderate
			1. Concur. A periodic review of each server's backup schedule and exclude lists will be performed beginning with the first quarter of FY08. In addition, the process for the maintenance of the exclude list will be documented and updates restricted.
			
			2. Concur. The initial process redesign will be completed by 12/15/07.

Findings	Recommended Action	Risk Management Information	Response
IS subsequently decided to reassess the backup needs for these servers. **Mainframe** • We determined that the mainframe was receiving scheduled backups. **Databases** • We determined the 379 Oracle, SQL and DB2 databases were receiving scheduled backups to tape. **Backup Policies** • Policies are rules that the backup software follows when backing up servers. A "full" policy is used to perform a complete backup of the server. We identified 201 full policies across 20 primary backup servers. Of those policies, three were inactive and ten were obsolete. IS plans to remove the obsolete policies. **Exclude Lists** • Exclude lists define files and/or directories that will not be backed up on a server. Our understanding is groups other than the Backup Group (i.e. System Administrators) have the ability to make changes to the exclude list. For nine servers, IS did not have supporting documentation for the exclusions. Other Observations • We believe management should consider an overall process design review to develop a			

Findings	Recommended Action	Risk Management Information	Response
better integrated and efficient backup and restore process. The review should address issues previously found in OIG audits, Summary of Aggregated Gap design control deficiencies (such as backup verification, controls implemented as a result of the backup failures), and the following observations: o There appears to be a lack of integration/communication between groups with key responsibilities in the backup process. o Multiple Service Levels (4) and DR Classes (4) may be contributing to a more complex environment than necessary. ▪ Customer have been able to choose a wide variety of combinations between service levels and DR classes (16 total combinations) ▪ IS has not yet synchronized applications and data based on service levels and DR classes (i.e., many database instances have data for applications that have two or more service levels). o Server roles were not always accurate in HPSD - three servers classified as production were actually retired.			