TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement

February 11, 2016

Reference Number: 2016-20-019

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

MANAGEMENT OVERSIGHT OF THE TIER II ENVIRONMENT BACKUP AND RESTORATION PROCESS NEEDS IMPROVEMENT

Highlights

Report issued on February 11, 2016

Highlights of Reference Number: 2016-20-019 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Inadequate backup and restoration of Tier II environment data could result in the loss of taxpayer or management information and unrecoverable data following a disaster. Effective management of the Tier II backup and restoration environment is crucial to ensure that information technology fully supports business operations by efficiently providing services to taxpayers.

WHY TIGTA DID THE AUDIT

The IRS Chief Technology Officer requested that TIGTA evaluate the Tier II backup and restoration process following an incident in which the IRS discovered that a backup did not exist when needed to restore a significant database. Our overall objective was to evaluate the effectiveness of the IRS's Tier II backup and restoration process.

WHAT TIGTA FOUND

The IRS is not effectively managing its Tier II environment backup and restoration process. For example, IRS management has not established goals and does not regularly collect sufficient performance metrics to monitor, measure, and report on the effectiveness of the process. The dashboard created to report on the completion status of backups is not sufficient.

TIGTA identified additional areas for improvement, including problem reporting and root cause analysis, standard operating procedures, and access control. Also, the IRS did not properly analyze, document, or take effective corrective actions in response to the database incident. As a result, management still does not have information to detect if a required backup is not created. Similarly, management does not routinely test restore of backups to ensure the integrity and reliability of the data. In addition, 28 (35 percent) of 81 Tier II backup software applications are at their end of life, which could result in a lack of vendor critical security and maintenance support. Likewise, 104 (100 percent) of the hardware equipment used in the Tier II backup environment is beyond its useful life and has critical deficiencies that should be addressed.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer establish goals and performance measures; implement a problem management process; create and implement a backup strategy that includes tests to restore databases; ensure that a root cause analysis is performed on known vulnerabilities and corrective actions are properly documented; develop standard operating procedures; and establish automated procedures to notify support personnel and system owners that backups have been completed. To improve the Tier II backup and restoration environment, TIGTA recommended that the Chief Technology Officer upgrade the software and aged hardware infrastructure, and develop specific guidelines that should be taken when equipment reaches its end of useful life.

The IRS agreed with 10 recommendations and partially agreed with three recommendations. The IRS agreed to establish goals and plans to implement performance measures and to use the measures to take appropriate corrective actions; implement the problem management process; revise standard operating processes and procedures; create and implement a backup strategy; review all privilege groups; establish automated notification procedures; upgrade hardware and software; and develop guidelines for when hardware reaches the end of its useful life. The IRS disagreed with parts of three recommendations, including using performance metrics to determine staffing needs and adding software compatibility to the *Infrastructure Currency* policy.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

February 11, 2016

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement (Audit # 201520027)

This report presents the results of our review of the effectiveness of the Internal Revenue Service's (IRS) Tier II backup and restoration process. This audit was performed at your request, is included in our Fiscal Year 2016 Annual Audit Plan, and addresses the IRS major management challenges of Achieving Program Efficiencies and Cost Savings, and Security for Taxpayer Data and Employees.

Management's complete response to this report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

DBA	Database Administrator
DMSS	Data Management Services and Support
DSA	Data Storage Administrator
IRS	Internal Revenue Service
TIGTA	Treasury Inspector General for Tax Administration
WRMS	Work Request Management System

Background

The Internal Revenue Service's (IRS) Chief Technology Officer requested that the Treasury Inspector General for Tax Administration (TIGTA) review the Tier II environment, specifically related to an incident of lost backup data on the Work Request Management System (WRMS). The WRMS tracks and controls information technology work requests from submission through completion, and maintains the status and assignment information. This system is owned and used by the IRS's Information Technology organization. Due to lost backup data, the WRMS could not be restored immediately when the database was inadvertently deleted.

The Tier II environment consists of non-mainframe servers. These servers run various operating systems, including versions of Microsoft Server, Linux, and UNIX. The servers may also operate as database, web, e-mail, and file servers, and provide a host of other important functions supporting the IRS network infrastructure. Some examples of important data stored within the Tier II environment include e-mails, personal and shared files, and taxpayer information.

The Information Technology organization's Enterprise Operations, Data Management Services and Support (DMSS) Division, Data Storage Branch, Data Protection Section is responsible for providing backup and restore services within the Tier II environment. The manager of the Data Protection Section leads a group of approximately 10 data storage administrators (DSA), who are each assigned servers at specific locations and are responsible for manually verifying the completion of backups throughout the server environment. A DSA will create a backup policy upon request from system administrators. A backup or restore occurs when the data on a server are being copied to or recreated from another media.[1] The backups generally run on a daily or weekly schedule. The IRS uses Symantec NetBackup to back up data in the Tier II environment.

This review was performed at the Enterprise Computing Centers in Martinsburg, West Virginia, and Memphis, Tennessee, and by contacting Information Technology organization personnel during the period of January through October 2015. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[1] See Appendix IV for glossary of terms.

Results of Review

The Internal Revenue Service Has Not Implemented Sufficient Internal Controls to Effectively Manage the Tier II Environment Backup and Restoration Process

Agencies and individual Federal managers must take systematic and proactive measures to develop and implement appropriate, cost-effective internal controls for results-oriented management; assess the adequacy of internal controls in Federal programs and operations; identify needed improvements; and take corrective actions. Internal controls are the organization, policies, and procedures used to reasonably ensure that programs achieve their intended results. Efficient and cost-effective management of the Tier II backup and restoration environment is crucial to ensuring that information technology fully supports business operations by efficiently providing services to taxpayers. Inadequate backup and restoration of Tier II environment data could result in the loss of taxpayer or management information, and could also result in data being unavailable for disaster recovery or business continuity.

The IRS is not effectively managing its Tier II environment backup and restoration process

In March 2015, the Enterprise Operations and Enterprise Services organizations presented to the Chief Technology Officer a briefing of the IRS's Tier II environment backup process that included key performance measures, such as the number of databases by type, number of failed backups per month, and number of restore requests. However, DMSS management, responsible for the IRS's Tier II backup and restoration process, has not established goals and does not regularly collect sufficient performance metrics to monitor, measure, and report on the effectiveness of the backup and restoration process. Information for the metrics has not been gathered on a regular basis as part of a management oversight program and is not used to identify and take actions on areas that are not performing as expected. The metrics included in the presentation were gathered only once for the purpose of preparing the Chief Technology Officer briefing. For example, the briefing showed a dedicated staff of 10 to monitor more than one million backups per month and to correct more than 44,000 failed backups per month in the Tier II environment. Furthermore, DMSS management does not use metrics to determine the root causes of the failed backups and implement effective corrective actions. Figure 1 provides additional information presented in the Chief Technology Officer briefing.

Figure 1: Tier II Backup Environment Metrics

Key Metrics	Calendar Year 2012	Calendar Year 2014	IRS Calculated Percentage Increase/Decrease	TIGTA Recalculated Percentage Increase/Decrease
Number of Restore Requests	310	487	36.3%	57.1%
DSA to Server Ratio	386	695	44.5%	80.1%
Number of Problem Tickets	700	1,251	44.0%	78.7%
Number of Servers Added	400	1,067	62.5%	166.8%
Number of DSA Employees	18	10	(80.0%)	(44.4%)

Source: IRS Information Technology Backup Process Overview And Infrastructure Refresh Options, March 2015.

While we did not verify the accuracy of the numbers in Figure 1, the percentages provided are incorrectly calculated. The miscalculation occurred because the IRS divided the difference between the amounts for Calendar Years 2012 and 2014 by the Calendar Year 2014 number, rather than the Calendar Year 2012 number. Based upon the new calculation, the number of servers added over the two-year period did not increase by 62.5 percent, but rather by 166.8 percent, more than two and one-half times the percentage increase reported. The incorrect calculations are considerable and may have a significant impact on the management of the backup and restoration program.

TIGTA's recalculation shows a 57.1 percent increase in the number of restore requests from Calendar Years 2012 to 2014; however, there is no corresponding root cause analysis to determine the reason for the increase or a corrective action plan. Similarly, the number of problem tickets increased 78.7 percent over the same two-year period. Further analysis is needed to identify specific problems causing the increase and to develop an action plan to correct the issues.

We also found that there is only one recurring report of the Tier II backup environment sent from the database administrators (DBA) and the DSAs to DMSS management. DMSS management created a Daily Backup Dashboard report in January 2015 as a corrective action following the WRMS incident to inform management, the DBAs, the DSAs, and system administrators on the completion statuses of backups. Prior to the creation of this report, no reporting existed for the backup process. However, we determined that this new dashboard is not sufficient for the following reasons:

- The dashboard contains only information on databases within the Tier II server environment. The success and failure of backups for applications, file and e-mail servers, and other information residing on servers are not reported on this dashboard.
- The dashboard does not provide the outcomes on the previous day's failures or trending information for analysis. Management is informed of failures each day but is not updated on the resolution of those failures in subsequent daily reports. The report also does not show trending analysis, such as the number of consecutive days a backup failed or the number of times a backup failed during the last three months.
- The dashboard does not contain any information on required backups that were inadvertently deleted or not created. The report shows only the statuses of backups that were run and whether they were successful. To illustrate, if a project has many databases, the DBA may not notice if one of the databases does not appear on the report.

We identified additional areas in which management of the backup and restoration process can be improved.

- **Backup successful and failure notification** – DMSS management does not have information to identify required backups that are not created. The DBAs explained that they can go directly to the database to determine if a backup was created. Some DBAs do this on a daily basis, while others do not perform this step. Still, other DBAs stated they have a daily report run that informs them of the status of their required backups. DMSS management stated that there was a checklist used by the DBAs to identify whether backups are created for a new or upgraded database. However, we determined that the checklist does not exist.

  Our review also determined that the backup software has the capability to notify personnel via e-mail of the completion statuses of backups and restores. This software could be used to notify system owners, system administrators, DMSS management, the DBAs, and the DSAs of successful completions and/or failures of backups.

- **Problem reporting and root cause analysis** – The DSAs are required to create Knowledge Incident/Problem Service Asset Management problem tickets for failed backups recorded on the daily dashboard. DMSS management has yet to retrieve and analyze the data to identify the root causes of failed backups and develop appropriate corrective actions. When TIGTA requested a Knowledge Incident/Problem Service Asset Management report of problem tickets for failed backups, DMSS management could not provide the report. Rather, each DBA provided a list of problem tickets they individually worked for failed backups. We received a list of 33 tickets for failed backups worked by the DBAs from January 2014 to June 2015. Management could not confirm the completeness of the list provided. DMSS management cannot effectively use the Knowledge Incident/Problem Service Asset Management system to analyze the failed backups because procedures have yet to be developed and implemented to ensure that all

failed backups are tracked and problem tickets are consistently prepared. Management also has not assigned responsibility to analyze the failed backups reported in problem tickets and recorded on the daily dashboard report for trends or root causes.

- **Formal procedures** – The DSAs do not have sufficient standard operating procedures to create routine backups consistently. For example, the DSAs may use different methods to create backups depending on the size of the data. The DSAs stated that they use professional judgment or communicate with other DSAs when unsure of appropriate procedures. Management has not developed adequate detailed procedures for the DSAs to perform routine backup duties. The lack of formalized procedures resulted in the DSAs applying varied methods to create or monitor backups.
- **Problem management process** – IRS standard operating procedures, *Enterprise Operations Problem Management Process*,[2] establish guidance on how repeat incidents should be addressed. The DSAs informed us of persistent problems that have caused recurring backup failures, but the DSAs did not initiate the problem management process. For example, an error in communication between the servers and the Symantec NetBackup software resulted in backups failing. One DSA stated this condition began when the IRS initially upgraded its e-mail servers and has worsened with more recent upgrades to its servers. In another example, repeated network connection drops at one Computing Center caused frequent failures in backups. In both instances, the DSAs only addressed the incidents of the failed backups and did not initiate the problem management process to determine and address the root cause. DMSS management does not provide proper oversight to ensure that the DSAs initiate the problem management process for repeat incidents. Not following the problem management process has resulted in persistent backup failures going uncorrected. As a result, the DSAs expend time and effort to routinely rerun failed backups caused by the same underlying issues.
- **Access control** – The IRS does not have sufficient access controls for personnel performing backup duties. Federal guidelines require organizations to specify authorized users of the information system, group and role membership, access authorizations, *i.e.*, privileges, and other attributes for each account. DMSS management did not identify all users who have permission to perform backup or restore responsibilities. We observed at least one DSA performing backup duties who was not identified as having backup rights. Also, we identified at least one group of administrators who had the capability of performing backup and restore duties who were not the DSAs. DMSS management could not fully explain how personnel, not part of the backup group, were granted the permissions to perform backup duties. Improper access controls increase the risk of unauthorized actions and could compromise the confidentiality, integrity, and availability of IRS data. Personnel who retain but do not require access privileges to

[2] IRS, *Enterprise Operations Problem Management Process Standard Operating Procedures* (Dec. 2014).

perform backup or restore duties could potentially violate separation of duties and least privilege requirements.

- **Backup management procedures and restore testing** – The Internal Revenue Manual and Tier II backup procedures and guidelines require that the DBAs shall periodically test backup copies of databases. Furthermore, effective backup management procedures should include periodic restore testing and confirming the integrity or viability of the backup media. However, DMSS management does not routinely test restore of backups to ensure the integrity and reliability of the data by performing restores. DMSS management only initiates test restores upon request. DMSS management also does not follow Internal Revenue Manual requirements for periodic restore testing. The DSAs and managers stated that there is an internal verification of data integrity immediately following the backup process and as part of disaster recovery exercises; however, these verifications are not a restore test. Without forming a strategy for backup restore testing, the IRS cannot be assured it will have reliable backup data when needed. The inability to restore databases or systems containing critical taxpayer information could damage the IRS's reputation and ability to accomplish its tax administration mission.

Office of Management and Budget, Circular A-123, *Management's Responsibility for Internal Control*,[3] provides requirements and guidance to Federal managers on improving the accountability and effectiveness of Federal programs and operations by establishing, assessing, correcting, and reporting on internal controls. Agencies and individual Federal managers must take systematic and proactive measures to develop and implement appropriate, cost-effective internal controls for results-oriented management; assess the adequacy of internal controls in Federal programs and operations; identify needed improvements; and take corrective actions. The Government Accountability Office, *Standards for Internal Control in the Federal Government*,[4] states that management uses performance measures to evaluate the effectiveness of Federal programs. DMSS management is not following Federal requirements for implementing internal controls, evaluating those controls, and measuring the effectiveness of the Tier II environment backup and restoration process. DMSS management also does not have a process or procedures to effectively confirm that all required backups are created or if a required backup no longer exists. There are no procedures that specify the DBAs are responsible to ensure that required backups are created and require the DBAs to use the same method to verify or ensure that routine backups are created consistently.

The lack of management information about the backup process contributed to a significant incident in December 2014 when a backup needed to restore the WRMS database, deleted in error, did not exist. The IRS's analysis of the incident determined that the backup for the

[3] Office of Management and Budget, Circular A-123, *Management's Responsibility for Internal Control* (Dec. 2004).
[4] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

database had not been created for four months prior to the condition being discovered. As a result, the system owner and information technology personnel expended significant resources restoring the data lost from the WRMS incident. The potential for these events to occur to other critical systems within the IRS still exists. The failure to restore a system containing taxpayer data could impact the IRS's ability to administer the tax code and cause a loss of taxpayer confidence in the agency.

Without effective internal controls, management will not have the necessary tools to meet its responsibility for effectively assessing and responding to risk, and accurately demonstrating the accomplishment of goals and objectives. As the number of systems and databases in the IRS's Tier II environment increases, it is crucial that management implement an effective system of internal controls to ensure that data are backed up and can be restored. When management information is not regularly collected and analyzed, DMSS management cannot use the information to initiate actions to improve the backup and restoration process. For example, the metrics show that while the number of servers, backups, and problem tickets has increased, there has been a 44.4 percent decrease in employees assigned to monitor and fix problems in these areas. DMSS management could use this information to determine an appropriate staffing level and to request additional resources. DMSS management stated that the lack of sufficient staffing is a significant challenge to effectively manage the Tier II backup and restoration process. Similarly, the lack of detailed procedures for the DSAs to perform routine backup duties creates a system that lacks consistent and repeatable processes, is undocumented, and is in a state of dynamic change.

Recommendations

The Chief Technology Officer should:

Recommendation 1: Establish goals and implement performance measures to determine the effectiveness of the backup and restoration process.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to establish goals and implement performance measures to determine the effectiveness of the backup and restoration process.

Recommendation 2: Use the performance measures to take appropriate corrective actions, as necessary, including determining and requesting the appropriate staffing level for the backup and restoration process.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS plans to use performance measures to take appropriate corrective actions, as necessary. The IRS disagreed that staffing levels can be determined by reviewing performance measures.

Office of Audit Comment: We disagree with the IRS's position to not use performance measures to determine staffing levels. We believe there is sufficient statistical evidence provided by the IRS produced key metrics in Figure 1 to reasonably determine staffing needs within the IRS's backup and restore environment. As shown in Figure 1, there is a 57.1 percent increase in the number of restore requests, an 80.1 percent increase in the DSA to server ratio, a 78.7 percent increase in the number of problem tickets related to backups and restores, a 166.8 percent increase in the number of servers requiring backups and restores, and a 44.4 percent decrease in the number of DSA staffing. With these levels of increase in the backup and restore workload and a significant decrease in staffing to handle the workload, we believe it is reasonable to determine the DSA staffing needs based on the metrics.

Recommendation 3: Ensure that Enterprise Operations organization management and employees are familiar with and implement the problem management process to identify and remediate the root causes of recurring incidents.

Management's Response: The IRS agreed with this recommendation. IRS Enterprise Operations managers plan to review all backup and restore problem management cases to ensure that the problem management process is followed and that the root cause is identified and remediated. The IRS states that all employees have been briefed on the proper uses of the problem management processes.

Recommendation 4: Revise processes and procedures, including managerial oversight responsibilities, to ensure that routine backup duties are consistently performed.

Management's Response: The IRS agreed with this recommendation. The IRS plans to revise processes and procedures, including managerial oversight responsibilities, to ensure that routine backup duties are consistently performed.

Recommendation 5: Create and implement a backup strategy that includes tests to restore databases and systems from backup data.

Management's Response: The IRS agreed with this recommendation. The IRS plans to revise and implement backup processes and procedures that include tests to restore databases and systems from backup data.

Recommendation 6: Identify and review all privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel are granted appropriate authorization.

Management's Response: The IRS agreed with this recommendation. The IRS states it has reviewed the privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel has appropriate authorization.

The IRS did not properly analyze, document, or take effective corrective actions in response to the WRMS backup incident

DMSS management did not sufficiently document details of the WRMS incident. Documentation of the incident consisted of only a short passage in a January 2015 briefing to the Chief Technology Officer on the backup process. The IRS briefing lists the following three major factors contributing to the loss of data that resulted from the failed backup of the WRMS database:

1. While addressing storage capacity needs, a system administrator overwrote the database, rather than allocating or compressing files to create more space. The system administrator did not follow IRS standard operating procedures.
2. When the database was upgraded on July 28, 2014, a DSA deactivated the backup policy of the old database and did not enable the backup policy for the new database. The DSA also did not follow IRS standard operating procedures.
3. The DBAs did not notice for four months that the database was not being backed up and status reports did not identify failures because the WRMS backup was not enabled.

Also, we determined that the IRS's analysis of the incident was not completely accurate. The WRMS database upgrade occurred in January 2014, rather than in July 2014 as reported in the Chief Technology Officer briefing. At that time, the backup policy for the upgraded database was enabled and successfully creating backups. On July 29, 2014, the DBA assigned to the database requested by e-mail that the DSA delete the old backup policy. The DSA responded to the request by deleting the only backup policy in place, believing this was the old policy. In doing so, the DSA deleted the backup policy for the upgraded database.

In addition, DMSS management did not implement effective corrective actions. As previously stated, in January 2015 management initiated use of a Daily Backup Dashboard report of failed and completed backups in response to the WRMS incident. Each DBA is required to review the report daily and address any failed backups for their assigned projects. They also are required to create a Knowledge Incident/Problem Service Asset Management problem ticket for each failed backup and ensure that the problem causing the failure is corrected and the backup is successfully created. DMSS management stated that this is the corrective action put in place to ensure that the DBAs will identify if a required backup is not created. However, there is no documentation supporting that this report is the corrective action for the WRMS incident, nor were the incident and corrective action tracked on a Plan of Action and Milestones, as required. Similarly, there are no written procedures on how the DBAs, the DSAs, and DMSS managers should use the report. As a result of not adequately and accurately analyzing the WRMS incident, management initiated a corrective action dashboard report of failed and completed backups that does not address the root cause of the incident.

Following the data loss incident, the WRMS system owner initiated actions to receive notification that database backups are completed and can be effectively restored. The system

owner now receives a daily report via e-mail confirming that the backup is completed for the previous day. The system owner also requested a test to restore the database from a backup. The test showed that the database was successfully restored. However, DMSS management has not initiated similar verification procedures on any other databases or systems. The absence of effective corrective actions to ensure that controls are in place to prevent backups from being deleted, and to alert personnel if required backups are not created, places the IRS at risk that this condition could occur again without being detected.

Recommendations

The Chief Technology Officer should:

Recommendation 7: Ensure that a root cause analysis is performed on known vulnerabilities, including the WRMS incident, and corrective actions are properly documented in a Plan of Action and Milestones.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS states it has a well-documented Incident Management and Problem Management process in place that is used to determine and document root causes and that this process was used to determine and fix the root cause of the WRMS incident. The IRS plans to continue to ensure that corrective actions identified for root causes are documented in appropriate information technology action plans.
>
> ***Office of Audit Comment:*** We disagree with the IRS's position that an adequate process was used to perform a root cause analysis and properly document corrective actions of the WRMS incident. We requested the IRS's documentation for performing its Incident Management and Problem Management process related to the WRMS incident. Documentation of the incident consisted of only a short passage in a January 2015 briefing to the Chief Technology Officer on the backup process. We determined that the IRS's analysis of the incident was not completely accurate and that DMSS management did not implement effective corrective actions in response to the WRMS incident. The IRS's root cause analysis did not identify that the incident occurred, in part, because there was no control in place to provide an alert when the WRMS database backup was not being created; therefore, the corrective actions taken did not address this root cause. There is also no documentation supporting that the corrective action taken was the result of the IRS performing its Incident Management and Problem Management process for the WRMS incident. In addition, the incident and corrective action was not tracked on a Plan of Action and Milestones, as required.

Recommendation 8: Develop standard operating procedures for the DBAs and the DSAs to establish standard methods when creating and deleting backup policies, and verifying backups are created.

Management's Response: The IRS agreed with this recommendation. The IRS plans to revise the standard operating procedures for DBAs and DSAs to establish standard methods when creating and deleting backup policies, and to verify that backups are created.

Recommendation 9: Establish automated procedures for sending status notifications to DMSS personnel and system owners confirming backups have been completed.

Management's Response: The IRS agreed with this recommendation. The IRS plans to establish procedures that will be automated, as appropriate, for sending status notifications to DMSS personnel and system owners confirming that backups have been completed.

Tier II Backup and Restoration Environment Software and Hardware Should Be Updated

The backup software has critical deficiencies that should be addressed

At the end-of-life date, vendors may no longer provide critical support, such as program updates, fixes, security patches, security alerts, patch updates, and general maintenance releases. We evaluated the currency of the IRS backup software based on vendor specified end-of-life dates. We identified 28 (35 percent) of 81 IRS backup software applications that are at their end of life.

We also evaluated the backup software for compatibility with applications and operating systems within the IRS Tier II environment. The software in use for backing up data on IRS exchange servers is currently NetBackup Enterprise 7.1; however, Symantec recommends[5] that the version be at least 7.5.0.5 to be considered compatible. We identified that 66 (88 percent) of 75 NetBackup applications and appliances are not compatible with all IRS application software and operating systems. With the IRS's planned upgrade to Windows Server 2012, Symantec's NetBackup Enterprise software will compound the compatibility issues and will not be supported until its NetBackup software is also upgraded.

The National Institute of Standards and Technology, Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*,[6] requires that information system components be replaced when support for the components is no longer available from the developer, vendor, or manufacturer. The IRS's use of software that has reached its end of life could result in a lack of vendor critical support and provide opportunities for hackers to exploit newly discovered weaknesses. DMSS management stated that the IRS lacks the resources, both

[5] Symantec NetBackup™ Database and Application Agent Compatibility List, June 1, 2015.
[6] National Institute of Standards and Technology, Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013).

budgetary and in modernized physical equipment, to update the software in use for its Tier II backup environment.

The IRS does not have a policy that provides guidance for keeping software current. The IRS has an initiative, *Infrastructure Currency*, which proposes that the agency maintain commercial software to be no more than one major release behind the latest version. Applying the IRS's initiative and the vendor's definition of a "major release," none of the backup software is more than one major release behind. However, software that may be only one major release behind could still be at its end of life depending on the vendor. It may also have compatibility issues with operating systems and applications currently used by the IRS, and no longer meet Federal requirements of being supported.

The hardware used in the backup environment is beyond its useful life and has critical deficiencies that should be addressed

The IRS has a policy to determine useful life; however, DMSS management stated that they apply a "5 year" rule to determine the end of useful life of its Tier II environment backup equipment by adding five years to the received date. While we recognize this is not an IRS policy, we applied this rule to gauge the maturity of IRS equipment in the Tier II backup environment. Applying this rule, we determined that 104 (100 percent) of the hardware equipment in the Tier II backup environment are past its "useful life." The hardware had received dates ranging from March 3, 2004, to September 1, 2010. However, we do not believe this is a full accounting of the IRS's inventory for its Tier II backup environment. During two site visits, we identified discrepancies between the hardware list provided by DMSS management and the location of the physical equipment. The IRS was unable to fully resolve the discrepancies and provide a complete and comprehensive list of the hardware equipment in the Tier II backup environment.

DMSS management is not effectively administering Tier II backup environment asset management and tracking all equipment from procurement to disposal. The IRS also did not adhere to its useful life policy for its Tier II backup equipment. Furthermore, there are no specific guidelines for actions that should be taken when equipment reaches its end of useful life.

Using outdated equipment increases risk within the backup environment. The DSAs reported that physical servers are outdated and cannot properly handle new software versions of Symantec NetBackup. The newer versions are necessary for better reporting functionality and greater compatibility with newer operating systems. The lack of hardware tracking inhibits the IRS's ability to effectively identify and manage the components of the backup and restore environment.

Recommendations

The Chief Technology Officer should:

Recommendation 10: Upgrade the software for the Tier II backup environment to meet Federal requirements and operational needs as resources are identified.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS plans to upgrade the Tier II backup software to the most current version, contingent upon funding, aligning with IRS processes and procedures to assess, and prioritize and implement currency-related upgrades.

Recommendation 11: Incorporate the IRS software modernization initiative, *Infrastructure Currency*, into written policies and guidelines for keeping software current. This policy should ensure that software is supported and compatible.

> ***Management's Response:*** The IRS partially agreed with this recommendation. The IRS states that the *Infrastructure Currency* initiative is an evolving effort and, as such, guidelines are still under development. Once fully developed, guidance will capture repeatable processes and intersections with established processes to assess, prioritize, and implement currency-related upgrades. The guidance will not address compatibility as that is already documented in existing Internal Revenue Manuals. Targeted completion date for *Infrastructure Currency* guidance is March 2017.
>
> ***Office of Audit Comment:*** We disagree with the IRS's position to not include software support and compatibility in the *Infrastructure Currency* guidance. If the IRS is going to fully develop guidance for the *Infrastructure Currency* initiative as stated, we believe that the guidance should include software support and compatibility. Software that is only one major release behind could be at its end of life depending on the vendor. It may also have compatibility issues with operating systems and applications currently used by the IRS, and it may no longer meet Federal requirements of being supported.

Recommendation 12: Develop specific guidelines for actions that should be taken when hardware reaches its end of useful life.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS states these guidelines are already in place and are used as part of the rust replacement strategy of the Sustaining Infrastructure program.

Recommendation 13: Upgrade the aged Tier II backup environment hardware infrastructure as resources are identified.

> ***Management's Response:*** The IRS agreed with the recommendation. The IRS plans to upgrade the aged Tier II backup environment hardware infrastructure, contingent upon funding, aligning with IRS processes and procedures to assess, prioritize, and implement currency-related upgrades.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the effectiveness of the IRS's Tier II backup and restoration process. To accomplish our objective, we:

I. Identified the policies and procedures that apply to the Tier II backup and restoration process.

A. Identified Federal requirements for the backup and restoration process. We conducted research of Federal sources, such as the Department of the Treasury, the National Institute for Standards and Technology,[1] the Government Accountability Office, and the Office of Management and Budget, to identify guidelines and requirements for agencies to implement and manage backup and restoration policies and procedures for information technology systems.

B. Identified IRS policies and procedures for implementing and managing a backup and restoration process. We researched the IRS's website (IRS.gov) to identify Internal Revenue Manual requirements applicable to the backup and restoration process.

C. Interviewed DMSS personnel to identify and obtain all standard operating procedures applicable to backup and restoration for the Tier II environment.

II. Evaluated management oversight of the Tier II backup and restoration process, including corrective actions taken in response to the WRMS database backup incident.

A. Determined how IRS management determines and monitors the effectiveness of the Tier II backup and restoration process.

B. Evaluated corrective actions taken in response to the WRMS database backup incident.

III. Evaluated the hardware and software used for the backup and restoration process.

A. Determined if the hardware in use is fit for the purpose of accomplishing the requirements of the Tier II backup and restoration process.

B. Determined if the software in use is fit for the purpose of accomplishing the requirements of the Tier II backup and restoration process.

[1] See Appendix IV for a glossary of terms.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: Office of Management and Budget and Government Accountability Office requirements and guidelines for implementing effective internal controls in Federal agencies, and National Institute of Standards and Technology and Internal Revenue Manual requirements for implementing backup and restoration controls. We evaluated these controls by interviewing management and personnel responsible for the Tier II backup and restoration process and reviewing relevant IRS documentation.

Appendix II

Major Contributors to This Report

Danny Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
John Ledford, Acting Director
Louis Lee, Acting Audit Manager
Jason McKnight, Lead Information Technology Specialist
Joan Bonomi, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Associate Chief Information Officer, Strategy and Planning
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
Enterprise Operations Organization	The part of the IRS Information Technology organization that provides server and mainframe computing services for all IRS business entities and taxpayers.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drives effective tax administration to ensure public confidence.
Knowledge Incident/Problem Service Asset Management System	An IRS application that maintains the complete inventory of information technology and non–information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications.
Least Privilege	The principle of allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Media	Data storage material divided into three broad categories according to the recording method: 1) magnetic, such as diskettes, disks, tapes, 2) optical, such as microfiche, and 3) magneto-optical, such as CDs and DVDs.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Office of Management and Budget	Assists the President in overseeing the preparation of the Federal budget and evaluates the effectiveness of agency programs, policies, and procedures, and works to make sure that agency reports, rules, testimony, and proposed legislation are consistent with the President's budget and with Administration policies.

Term	Definition
Performance Measures	A means of evaluating an entity's performance in achieving objectives.
Plan of Action and Milestones	A document of the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities. The document is prepared for both systems and programs.
Symantec NetBackup	Symantec describes the NetBackup Platform as a holistic backup and recovery solution that is optimized for virtually any workload, whether physical, virtual, arrays, or big data, and delivers truly flexible target storage options, whether tape, third-party disk, appliances, including the NetBackup Deduplication Appliances and Integrated Backup Appliances, or cloud.

Appendix V

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

CHIEF TECHNOLOGY OFFICER

JAN 12 2016

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement (Audit #201520027) (e-trak # 2016-76418)

Thank you for the opportunity to review the audit report on the IRS's backup and restoration process of the Tier II environment.

We requested this audit as part of our commitment to effectively manage Tier II backup and restore services, and consistently apply adequate controls to prevent the loss of taxpayer and management information. During the course of the audit, we shared with the audit team several actions we have taken to address deficiencies identified in the audit report. Our actions include: establishing plans to upgrade backup software and hardware, creating a backup dashboard for all mission critical databases, and implementing procedures for making changes to backup policies and monitoring backup databases for completion.

We generally agree with the recommendations. However, we would like to point out that significant budget and resource constraints have challenged our efforts to modernize and maintain the computing infrastructures and associated processes that support the IRS's backup and restore requirements. Notwithstanding this challenge, we remain committed to providing the best backup and restore services possible. We appreciate the guidance and information you have provided.

Attached is our complete corrective action plan that addresses each recommendation. If you have any questions, please contact me at (240) 613-9373 or a member of your staff may contact Carmelita White, Senior Manager, Program Oversight at (240) 613-2191.

Attachment

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

RECOMMENDATION #1: Establish goals and implement performance measures to determine the effectiveness of the backup and restoration process.

CORRECTIVE ACTION #1: We agree with this recommendation. The IRS will establish goals and implement performance measures to determine the effectiveness of the backup and restoration process.

IMPLEMENTATION DATE: May 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: Use the performance measures to take appropriate corrective actions, as necessary, including determining and requesting the appropriate staffing level for the backup and restoration process.

CORRECTIVE ACTION #2: We partially agree with this recommendation. The IRS will use performance measures to take appropriate corrective actions, as necessary. We disagree that staffing levels can be determined by reviewing performance measures.

IMPLEMENTATION DATE: June 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #3: Ensure that Enterprise Operations organization management and employees are familiar with and implement the problem

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

management process to identify and remediate the root causes of recurring incidents.

CORRECTIVE ACTION #3: We agree with this recommendation. IRS Enterprise Operations managers are reviewing all backup and restore problem management cases to ensure the problem management process is followed and that root cause is identified and remediated. All employees have been briefed on the proper uses of the problem management processes.

IMPLEMENTATION DATE: Completed December 4, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: Revise processes and procedures, including managerial oversight responsibilities, to ensure that routine backup duties are consistently performed.

CORRECTIVE ACTION #4: We agree with this recommendation. The IRS will revise processes and procedures, including managerial oversight responsibilities, to ensure that routine backup duties are consistently performed.

IMPLEMENTATION DATE: June 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #5: Create and implement a backup strategy that includes tests to restore databases and systems from backup data.

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

CORRECTIVE ACTION #5: We agree with this recommendation. The IRS will revise and implement backup processes and procedures that include tests to restore databases and systems from backup data.

IMPLEMENTATION DATE: June 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #6: Identify and review all privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel are granted appropriate authorization.

CORRECTIVE ACTION #6: We agree with this recommendation. The IRS reviewed the privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel had appropriate authorization.

IMPLEMENTATION DATE: Completed June 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #7: Ensure that a root cause analysis is performed on known vulnerabilities, including the WRMS incident, and corrective actions are properly documented in a Plan of Action and Milestones.

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

CORRECTIVE ACTION #7: We partially agree with this recommendation. We have a well-documented Incident Management and Problem Management process in place that is used to determine and document root cause. This process was used to determine and fix the root cause of the WRMS incident. We will continue to ensure that corrective actions identified for root causes are documented in appropriate IT action plans.

IMPLEMENTATION DATE: Completed January 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #8: Develop standard operating procedures for DBAs and DSAs to establish standard methods when creating and deleting backup policies, and verifying backups are created.

CORRECTIVE ACTION #8: We agree with this recommendation. The IRS will revise the standard operating procedures for DBAs and DSAs to establish standard methods when creating and deleting backup policies, and verifying backups are created.

IMPLEMENTATION DATE: June 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #9: Establish automated procedures for sending status notifications to DMSS personnel and system owners confirming backups have been completed.

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

CORRECTIVE ACTION #9: We agree with this recommendation. The IRS will establish procedures which will be automated, as appropriate, for sending status notifications to DMSS personnel and system owners confirming backups have been completed.

IMPLEMENTATION DATE: June 25, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #10: Upgrade the software for its Tier II backup environment to meet Federal requirements and operational needs as resources are identified.

CORRECTIVE ACTION #10: We agree with this recommendation. The IRS will upgrade the Tier II backup software to the most current version, contingent upon funding, aligning with IRS processes and procedures to assess, prioritize and implement currency-related upgrades.

IMPLEMENTATION DATE: December 24, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #11: Incorporate the IRS software modernization initiative, *Infrastructure Currency*, into written policies and guidelines for keeping software current. This policy should ensure that software is supported and compatible.

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

CORRECTIVE ACTION #11: The IRS partially agrees with this recommendation. The Infrastructure Currency initiative is an evolving effort and as such guidelines are still under development. Once fully developed, guidance will capture repeatable processes, and intersections with established processes to assess, prioritize, and implement currency-related upgrades. This guidance will not address compatibility as this is already documented in existing IRMs. Targeted completion date for Infrastructure Currency guidance is March 2017.

IMPLEMENTATION DATE: March 25, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Program Management Office

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #12: Develop specific guidelines for actions that should be taken when hardware reaches its end of useful life.

CORRECTIVE ACTION #12: We agree with this recommendation. These guidelines are already in place and are used as part of rust replacement strategy of the Sustaining Infrastructure program.

IMPLEMENTATION DATE: Completed October 19, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #13: Upgrade the aged Tier II backup environment hardware infrastructure as resources are identified.

CORRECTIVE ACTION #13: We agree with the recommendation. The IRS will upgrade the aged Tier II backup environment hardware infrastructure, contingent upon funding, aligning with IRS processes and procedures to assess, prioritize and implement currency-related upgrades.

Attachment

Draft Audit Report – Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement
(Audit #201520027) (e-trak # 2016-76418)

IMPLEMENTATION DATE: December 24, 2016

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: The IRS will enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.