



*Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved*

**May 3, 2012**

**Reference Number: 2012-20-041**

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](mailto:TIGTACommunications@tigta.treas.gov)

Website | <http://www.tigta.gov>



## HIGHLIGHTS

### **DISASTER RECOVERY TESTING IS BEING ADEQUATELY PERFORMED, BUT PROBLEM REPORTING AND TRACKING CAN BE IMPROVED**

## Highlights

**Final Report issued on May 3, 2012**

Highlights of Reference Number: 2012-20-041 to the Internal Revenue Service Chief Technology Officer.

### **IMPACT ON TAXPAYERS**

Disaster recovery planning is a coordinated strategy for recovering computer systems following a disruption. By testing disaster recovery plans, recovery problems can be identified and corrected before an actual disruption occurs. The IRS is adequately planning and conducting disaster recovery tests, but IRS reporting of problems identified during the tests and the tracking of progress to implement recommendations made at the conclusion of the tests need to be improved. Effective disaster recovery capabilities are critical to ensure that key information systems can be recovered with minimal disruption to the critical IRS business processes they support. The data and services provided by these systems are also needed by Congress, the Department of the Treasury, tax professionals, taxpayers, and other Government agencies.

### **WHY TIGTA DID THE AUDIT**

During this audit, TIGTA observed and/or reviewed IRS disaster recovery tests. The IRS is required to conduct disaster recovery tests on its most critical computer systems. Disaster recovery testing is conducted to test the IRS's ability to recover major computer systems at one Computing Center to another Computing Center. This review was requested by the Cybersecurity organization and is also part of our statutory requirements to annually review the adequacy and security of IRS technology.

### **WHAT TIGTA FOUND**

The IRS is adequately planning and conducting disaster recovery tests of critical current production environment computer systems and is performing disaster recovery exercises and tests on the Customer Account Data Engine 2 system as it is being developed.

However, the IRS can improve disaster recovery test problem reporting and tracking. TIGTA found that problem tickets used by the IRS for identifying, resolving, and tracking problems encountered during the tests were not created for several problems. In addition, reports prepared by the IRS during the disaster recovery tests used to track the progress and problems it encountered in recovering systems did not have complete information on many of the processes run and problems identified during the tests. Finally, the IRS did not have a process for closely and formally tracking the implementation of the less serious recommendations it made at the conclusion of the disaster recovery tests. During the course of the audit, TIGTA auditors informed the IRS of the need to track these recommendations, and the IRS recently developed a tracking worksheet.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the Associate Chief Information Officer, Cybersecurity, 1) revise reports the IRS prepares during disaster recovery tests to include required entries for references to problem tickets and 2) create a process for reviewing the completeness of problem tickets and reports prepared during the tests to help ensure that they contain complete information.

In its response to the report, the IRS agreed with TIGTA's recommendations. The IRS 1) revised its disaster recovery test reports to require entries for references to problem tickets and 2) created a process for reviewing the completeness of problem tickets and reports.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

May 3, 2012

**MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER**

*Michael R. Phillips*

**FROM:**

Michael R. Phillips  
Deputy Inspector General for Audit

**SUBJECT:**

Final Audit Report – Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved (Audit # 201120024)

This report presents the results of our review of disaster recovery testing activities. The overall objective was to observe Internal Revenue Service (IRS) disaster recovery testing to determine whether the IRS is adequately testing its capability to recover major computer systems from one Computing Center to another and whether systems can be successfully recovered. This review was requested by the Cybersecurity organization.<sup>1</sup> This review addresses the major management challenge of Security for Taxpayer Data and Employees, is part of our statutory requirements to annually review the adequacy and security of IRS technology, and is included in our Fiscal Year 2012 Annual Audit Plan.

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

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

---

<sup>1</sup> See Appendix IV for a glossary of terms.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

## *Table of Contents*

<b>Background</b> .....	Page 1
<b>Results of Review</b> .....	Page 3
Disaster Recovery Tests Are Being Adequately Planned and Conducted, and Exercises and Tests Were Performed During the Development of the Customer Account Data Engine 2 System .....	Page 3
Disaster Recovery Test Problem Reporting and Tracking Can Be Improved .....	Page 7
<u>Recommendations 1 and 2:</u> .....	Page 11
<b>Appendices</b>	
Appendix I – Detailed Objective, Scope, and Methodology .....	Page 12
Appendix II – Major Contributors to This Report .....	Page 14
Appendix III – Report Distribution List .....	Page 15
Appendix IV – Glossary of Terms .....	Page 16
Appendix V – Management’s Response to the Draft Report .....	Page 18



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

## *Abbreviations*

CADE 2	Customer Account Data Engine 2
IMF	Individual Master File
IRS	Internal Revenue Service
ITAMS	Information Technology Asset Management System
KISAM	Knowledge, Incident/Problem, Service and Asset Management
NIST	National Institute of Standards and Technology



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

## *Background*

The ability of the Internal Revenue Service (IRS) to carry out its mission and provide key taxpayer service and enforcement operations is heavily dependent on an extensive network of computer systems spread across the country. During Fiscal Year<sup>1</sup> 2010, the IRS reported that its computer systems processed more than 230 million returns, provided more than \$467 billion in refunds, collected more than \$2.3 trillion in taxes (93 percent of the Federal Government's receipts), received more than 305 million visits to its websites, and received more than 98 million electronically filed individual income tax returns. In addition to the IRS needing these systems to administer the Nation's tax system, data and services provided by these systems are needed by Congress, the Department of the Treasury, tax professionals, taxpayers, and other Government agencies.

Significant events, such as the terrorist attacks on September 11, 2001, and Hurricane Katrina in August 2005, have emphasized the need for organizations to have plans in place that will ensure essential operations can continue during a wide range of emergencies. Disaster recovery is an organization's ability to respond to a disruption in services by implementing a plan to restore critical business functions within the stated disaster recovery goals. Disaster recovery planning<sup>2</sup> is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of information systems, computer operations, and data. If the IRS does not sufficiently test disaster recovery plans in accordance with policies and guidance, the risk increases that critical systems and the business processes supported by these systems may not be successfully recovered in a timely manner after a disruption. This would severely impact the ability of the IRS to carry out its mission. Testing of disaster recovery capabilities is a way of identifying deficiencies in disaster recovery plans, procedures, and training. By effectively testing disaster recovery plans, problems can be identified and corrected before an actual disruption occurs.

The Federal Information Security Management Act of 2002<sup>3</sup> and Office of Management and Budget mandates require agencies to establish an information technology disaster recovery planning and testing program to ensure that computer systems can be recovered in a timely manner after a disruption. Pursuant to its responsibilities under the Federal Information Security Management Act, the National Institute of Standards and Technology (NIST) developed standards and guidelines that Federal agencies are required to use in developing, conducting, and evaluating disaster recovery tests. The Department of the Treasury requires bureaus to develop

---

<sup>1</sup> See Appendix IV for a glossary of terms.

<sup>2</sup> Information technology disaster recovery planning is also referred to as contingency planning. Because universally accepted definitions are not available, throughout this report we used the term disaster recovery.

<sup>3</sup> 44 U.S.C. §§ 3541 – 3549.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

and implement a robust, cost-effective information technology security program that includes disaster recovery testing.

NIST and IRS policies require the IRS to conduct disaster recovery testing on its most critical computer systems, while less critical systems receive less rigorous disaster recovery exercises. Disaster recovery testing is conducted in as close to an operational environment as possible using components or systems used to conduct daily operations. Disaster recovery testing is designed to evaluate the IRS's readiness to cutover, relocate, restore, or rebuild its major systems and applications operating at one Computing Center to another Computing Center. To plan for a disaster recovery test, objectives and scope are defined and checklists, test plans, and other test documentation materials are developed. As the test is conducted, observations, notes, and forms are completed. At the end of a disaster recovery test, results are recorded, lessons learned are documented, corrective action plans are initiated, and disaster recovery plans are updated.

In a previous audit,<sup>4</sup> we reviewed the IRS's progress in completing its corrective actions on the seven components of its disaster recovery material weakness<sup>5</sup> and determined that corrective actions for the component on exercising and testing disaster recovery plans were being adequately completed. During this disaster recovery testing audit, we observed and/or reviewed IRS disaster recovery tests that took place in July, August, and October 2011.

This review was performed at the Cybersecurity organization's Disaster Recovery Testing Exercise and Evaluation offices in Martinsburg, West Virginia, and Memphis, Tennessee, during the period August 2011 through January 2012. 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.

---

<sup>4</sup> Treasury Inspector General for Tax Administration, Ref. No. 2011-20-060, *Corrective Actions to Address the Disaster Recovery Material Weakness Are Being Completed* (June 2011).

<sup>5</sup> In March 2005, the IRS declared its disaster recovery program a material weakness in accordance with the Federal Managers' Financial Integrity Act of 1982 [31 U.S.C. §§ 1105, 1113, 3512 (2000)]. The Federal Managers' Financial Integrity Act requires each Federal agency to conduct annual evaluations of its systems of internal accounting and administrative control. Each agency is also required to prepare an annual report for Congress and the President that identifies material weaknesses and the agency's corrective action plans and schedules.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

## *Results of Review*

### ***Disaster Recovery Tests Are Being Adequately Planned and Conducted, and Exercises and Tests Were Performed During the Development of the Customer Account Data Engine 2 System***

NIST and IRS disaster recovery testing policies and requirements cite the need to adequately plan and conduct disaster recovery tests and to perform disaster recovery exercises and tests as systems are being developed. The IRS is adequately planning and conducting disaster recovery tests of critical current production environment computer systems and is performing disaster recovery exercises and tests on the Customer Account Data Engine 2 (CADE 2) system as it is being developed.

#### ***Disaster recovery capability of critical current production environment computer systems is being adequately tested***

NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for Information Technology Plans and Capabilities*, cites the need to adequately plan disaster recovery tests. During the planning phase, the disaster recovery test is designed and test documentation is prepared. Appropriate planning meetings are held, the scope and objectives are established, specific tests and test cases are developed, the use of tools is determined, and test plans and guides are developed. If feasible, the plan should require that the test be done using components or systems used to conduct daily operations. To help plan the disaster recovery test, the IRS has created a *Disaster Recovery Test Plan Template*. This template contains the test's general objectives; general information such as the dates, call in number, and scenario; the results of any planning meetings that were held; test schedule and test scope; recovery time objectives; test participants; and responsibilities for test execution and summarization. To help plan the test cases, the IRS has created the *Test Case Daily Action Report Template*, which is prepared for each system that will be tested. This template contains the overall test objectives for each system to be recovered, the specific steps that will be performed for each system, and test cases for each system specifying equipment and personnel needs, goals, success criteria, and deliverables.

NIST Special Publication 800-84 and Internal Revenue Manual 10.8.62, *Information Technology Contingency Plan and Disaster Recovery Testing, Training, and Exercise Program*,<sup>6</sup> cite the need to adequately conduct disaster recovery tests. Disaster recovery tests begin with a scenario

---

<sup>6</sup> IRM 10.8.62 (Feb. 28, 2009).



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

containing the cause of the disaster, the systems and disaster recovery plans to be activated, the name of the alternate facility, the unavailability of staff at the damaged site, and other important information and rules on conducting the test. IRS test leaders are required to conduct at least two status meetings with the recovery staff each day, and independent observers are assigned to review and record recovery activities. Only the latest versions of disaster recovery plans are to be used to recover the systems. Staff from the production site should not be allowed to assist with recovery at the alternate site during a disaster recovery test because in a worst case real disaster those persons might not be available. Lessons learned from previous tests are built into subsequent tests to both improve the recovery and the testing process. As the test is conducted, disaster recovery staff enters results of the testing into the *Test Case Daily Action Report*.

We determined the disaster recovery tests conducted in July, August, and October 2011 were adequately planned. Specifically, we found:

- *Disaster Recovery Test Plans* were properly prepared with the test's objectives, scope, systems, scenario, instructions, recovery time objectives, and other necessary information.
- *Test Case Daily Action Reports*<sup>7</sup> were populated with the recovery activities, test cases, and job runs that will be tracked during the test with start and stop times.
- Systems were to be restored on actual production systems at the recovery site.

We also determined testing procedures were adequately followed for the August and October 2011 disaster recovery tests. Specifically, we found:

- In the August 2011 test, the disaster declaration, rules, and instructions were announced. Because the October 2011 test was limited in scope, a disaster declaration was not required.
- The daily status meetings reviewed progress and discussed and resolved problems.
- The *Disaster Recovery Test Plan* and the *Test Case Daily Action Report* were used to track process and job runs and also to ensure test objectives for each system were fulfilled.
- Other testing requirements were adhered to, such as using only the latest copy of the disaster recovery plan, not allowing staff at the "disaster site" to participate in any recovery activity unless stipulated in the disaster recovery test scenarios, focusing on the lessons learned from the previous disaster recovery test, and Cybersecurity organization staff acting as an independent observer and recorder.

---

<sup>7</sup> See definition on page 8.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

Generally, systems and applications were successfully recovered within recovery time objectives during the July and August 2011 tests. However, the recovery of a mainframe computer experienced significant problems during the July 2011 test. Because backup tapes had not been made, critical database subsystems could not be recovered until new backup tapes were created by the disaster site during the test. Five application databases were not recoverable, and much of the batch processing could not be performed.

The October 2011 test was a limited test that focused on the problems that occurred in recovering the mainframe computer in the July 2011 test. The October 2011 test resulted in significant improvements to the problems experienced during the July 2011 test.

**CADE 2 disaster recovery exercises and tests are being performed as the system is being developed**

NIST Special Publication 800-34, *Contingency Planning Guide for Federal Information Systems*, requires that initial disaster recovery exercises and tests be performed during the implementation phase of the Software Development Life Cycle to validate Information System Contingency Plan recovery procedures.

Disaster recovery exercises consist of Table Top Exercises and Functional Exercises. Table Top Exercises are discussion-based (walkthrough) exercises that do not involve deploying or recovering systems, equipment, or resources. Personnel meet to discuss their roles during an emergency and their responses to a particular emergency. The participants validate the content of the plan and related policies and procedures in the context of a particular emergency situation. Functional Exercises are more extensive than Table Top Exercises, requiring the event to be simulated. The exercises are designed to test procedures and assets involved in one or more functional aspects of the disaster recovery plan, such as backup retrieval, reading backup data, and validation of off-site storage.

Disaster recovery tests are conducted in as close to an operational environment as possible using components or systems used to conduct daily operations. The scope of testing can range from individual system components or systems to comprehensive tests of all systems and components that support a disaster recovery plan. These tests are designed to evaluate IRS readiness to cutover, relocate, restore, or build IRS systems. Disaster recovery tests involve activities such as cutovers from one platform or system to another, relocation of systems, or recovery of platforms and their hosted applications.

The CADE 2 is a vital IRS modernization effort and foundational component of the IRS's technology strategy that builds on the foundation of the current CADE. It is one of the IRS's top priority information technology investments. Its successful implementation is essential to reach the IRS's vision for tax administration. The CADE 2 will provide state-of-the-art individual taxpayer account processing and technologies to improve service to taxpayers and enhance IRS tax administration capabilities. It will provide faster refunds for millions of individual taxpayers and faster payment postings, account updates, and taxpayer notices. The CADE 2 will integrate



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

the CADE and the Individual Master File (IMF) into a single taxpayer processing system. It will also provide a single database that will improve user access to accurate and timely data. The CADE 2 will be implemented in phases. The first phase, called Transition State 1, is scheduled to be delivered for the 2012 Filing Season and will implement daily IMF processing. Daily processing will provide more accurate, timely data to frontline IRS employees and is expected to allow the IRS to update and settle accounts more quickly.

The IRS has developed a draft *CADE 2 Program Disaster Recovery Design Plan*. This document shows CADE 2 disaster recovery logical design, infrastructure, cost and sizing estimates, and other disaster recovery considerations. The CADE 2 has nine core components, and the IRS will be implementing two new types of disaster recovery technologies for six of them. These two new technologies are Virtual Tape Replication and Storage-Based Asynchronous Replication.

Virtual Tape Replication, instead of traditional backup tape, will be used because the CADE 2 IMF Daily Processing core component will process IMF data daily instead of weekly. To accommodate the backing up of IMF files that are processed daily, the IRS will implement a disaster recovery solution using International Business Machines Corporation's virtual tape replication product called gridding. Gridding is a technology that makes it possible to save data as if it were being stored on tape, although it is actually being stored on hard disk or another medium. Each day, gridding will transmit over the network IMF daily processing data from the Virtual Tape Library in the Martinsburg Computing Center to the Memphis Computing Center recovery site.

International Business Machines Corporation's Global Mirror storage-based asynchronous data replication is a solution that the IRS will use to replicate production data that will be transferred over the network from the Martinsburg Computing Center to the Memphis Computing Center recovery site for six CADE 2 core components. Asynchronous replication is a technique for replicating data between file systems in which the system being replicated can continue to be changed without having to wait for the remote system to have recorded changes previously transmitted by the system being replicated. An example of a CADE 2 core component that will be replicated using Global Mirror is the CADE 2 Database Implementation, which contains IMF data. The entire Martinsburg Computing Center CADE 2 database will initially be replicated to the Memphis Computing Center recovery site, after which only changes made to the database will be replicated on a daily basis.

The IRS has performed disaster recovery exercises and tests on the gridding and Global Mirror disaster recovery solutions and reported on the results of these exercises and tests in the draft *CADE 2 Disaster Recovery Testing Reports Overview* for Transition State 1, Enterprise Life Cycle Milestone 4b. The main purpose of these exercises and tests was to verify, prior to the implementation of the CADE 2, that CADE 2 disaster recovery solutions are ready for use. Disaster recovery exercise and test results in the IRS's report have confirmed the ability of these two solutions to successfully replicate production data from the Martinsburg Computing Center



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

to the Memphis Computing Center recovery site. The following disaster recovery exercises and tests were performed (in order of complexity).

- On October 20, 2011, the IRS performed a Table Top Exercise on gridding and Global Mirror replication procedures for recovering the Martinsburg Computing Center IMF and mainframe systems in the Memphis Computing Center recovery site. The exercise identified changes needed to disaster recovery procedures and other action items.
- In September 2011, the IRS performed a Functional Exercise on gridding replication. The exercise confirmed that virtual tape files initially sent and update files subsequently sent by the gridding solution in the Martinsburg Computing Center were successfully received by the gridding solution in the Memphis Computing Center recovery site.
- On October 7, 2011, the IRS completed a Functional Exercise on Global Mirror replication. The exercise confirmed that test volumes for the Martinsburg Computing Center IMF and mainframe systems initially sent and update files subsequently sent by Global Mirror in the Martinsburg Computing Center were successfully received by the Memphis Computing Center recovery site.
- On November 4, 2011, the IRS completed a Disaster Recovery Test on gridding and Global Mirror replication. The test confirmed the ability to restore the Martinsburg Computing Center IMF and mainframe systems in the Memphis Computing Center recovery site using gridding and Global Mirror file replication.

The IRS has also performed an initial disaster recovery test of the CADE 2 database as it was being loaded. In late November 2011, the IRS performed a test which confirmed that the files were backed up and reconciled. The IRS reported that the test successfully compared production files to recovery files and matched record counts to confirm the backed up files.

The IRS is planning to conduct a Computing Center to Computing Center disaster recovery test in Calendar Year 2012, at which time the CADE 2 production system in the Martinsburg Computing Center will be tested for recovery in the Memphis Computing Center recovery site.

### ***Disaster Recovery Test Problem Reporting and Tracking Can Be Improved***

NIST, Department of the Treasury, and IRS disaster recovery testing policies and requirements cite the need to report on testing problems and the status of testing processes and to track recommendations to improve disaster recovery capabilities. The IRS can improve the following areas of disaster recovery test problem reporting and tracking during the execution phase of disaster recovery tests.

- Problem tickets used by the IRS for identifying, resolving, and tracking problems encountered during the tests were not created for many problems.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

- Reports prepared by the IRS during the disaster recovery tests to track the progress and problems encountered in recovering systems did not have complete information on many of the problems and the processes run during the test.
- The IRS did not have a process for closely and formally tracking the implementation of the less serious recommendations made at the conclusion of the disaster recovery tests.

**Information Technology Asset Management System (ITAMS) ticket reporting and Test Case Daily Action Reports can be improved**

NIST Special Publication 800-84 states that reporting on disaster recovery testing should determine how well tested systems or components functioned. The introduction to the disaster recovery testing report should document background information about the test, such as the scope, objectives, and tests. The report should also document observations made by the test team during the test, lessons learned during the test, and recommendations for enhancing the disaster recovery plan that had its components or systems tested, along with associated procedures and components.

Internal Revenue Manual 10.8.62 requires that several reports be completed before, during, and after disaster recovery testing. These reports evaluate disaster recovery test results and identify weaknesses and corrective actions to improve IRS preparedness.

1. The *Test Case Daily Action Report* contains the overall disaster recovery test objectives for each system to be recovered; the specific steps that will be performed for each system; test cases for each system specifying equipment and personnel needs, goals, success (outcome) criteria, and deliverables; and the designation of the disaster recovery site executive as the person to decide an early termination and termination criteria. A completed *Test Case Daily Action Report* should indicate the start and stop time of each process, file, or job run; whether it was completed with or without interruption; a description of the interruption; a description of the corrective action used to complete the interruption; and whether a problem encountered in performing a test case required an update to the disaster recovery plan. The *Test Case Daily Action Report* is prepared by Enterprise Operations organization staff during the disaster recovery test.
2. The *Vulnerabilities Matrix Report* is prepared by the Cybersecurity organization and contains information on the problems that were reported in ITAMS tickets during the disaster recovery test. The ITAMS is a centralized database for incident management. The IRS requires that ITAMS tickets be created for all problems that occur during a disaster recovery test so that problems can be properly identified, resolved, and tracked, and disaster recovery plans can be revised if needed. The IRS also requires that ITAMS tickets created during a disaster recovery test contain detailed problem and problem resolution descriptions. Disaster scenario scripts that the IRS uses during disaster recovery tests stress that ITAMS tickets must contain detailed problems and resolutions.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

The ITAMS was replaced with the Knowledge, Incident/Problem, Service and Asset Management system (KISAM) on October 1, 2011.

3. The *Detailed Daily Observation Report* is prepared by the Cybersecurity organization and contains detailed recordings of the daily status meetings that take place during the disaster recovery test. It also contains other observations.
4. The *Executive Overview Report* is prepared by the Cybersecurity organization and contains the disaster recovery test's scenario, overall recovery results, recovery directives, test objectives, scope, accomplishments, findings, recommendations, and actions needed to correct weaknesses to specific computer systems.

The *Detailed Daily Observations Report* for the July 2011 disaster recovery test and the *Draft Detailed Daily Observations Report* for the August 2011 test contained substantial notes on the daily status meetings that took place on each day of the recovery, covered the discussions on each system that was being recovered, and contained Cybersecurity organization observations.

The *Executive Overview Report* for the July 2011 disaster recovery test and the *Draft Executive Overview Report* for the August 2011 test contained key information on the test's scope, objectives, tests, observations, lessons learned/findings, and recommendations, as suggested in NIST Special Publication NIST 800-84.

While the IRS prepared 46 ITAMS tickets during the August and October 2011 disaster recovery tests, tickets were not prepared for 10 problems. For eight of the 10 problems, the *Test Case Daily Action Report* indicated a problem, but an ITAMS ticket had not been prepared.

Many problems reported in *Test Case Daily Action Reports* and ITAMS tickets shown in the *Vulnerabilities Matrix* and *Shift Turnover Reports* for the July and August 2011 tests did not adequately describe the problems or interruptions that occurred or describe how the problems or interruptions were resolved. For example, the IRS prepared 105 ITAMS tickets during these two disaster recovery tests, but 20 tickets did not contain adequate descriptions of the problems or interruptions or describe how they were resolved. Sixty-four problems reported in the *Test Case Daily Action Reports* for these two tests did not contain adequate descriptions of the problems or interruptions or describe how they were resolved.

Other sections of the *Test Case Daily Action Reports* for the July and August 2011 disaster recovery tests were also incomplete. For 178 of the processes and jobs listed in the *Test Case Daily Action Reports*, there was no indication whether the processes or jobs were or were not completed or were completed with or without an interruption. For 111 of the processes or jobs listed in the *Test Case Daily Action Reports* that encountered a problem, there was no indication whether an update to the disaster recovery plan was or was not needed.

ITAMS tickets were not prepared and ITAMS tickets and *Test Case Daily Action Reports* were incomplete because they are prepared during the disaster recovery test. At this time, the technical employees who prepare these reports are concentrating on performing steps necessary



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

to continue recovering the systems. These reports are generally available at the completion of the disaster recovery test and are not revised or updated after the test is completed. Another reason why ITAMS tickets were not prepared could be that the template for the *Test Case Daily Action Report* lacks a column for entering the ITAMS ticket number related to a test case problem or for providing a reason why a ticket is not needed. Such a column would facilitate a repetitive process for creating necessary ITAMS tickets. Such a column would also be helpful in understanding the problems and the corrective actions because it would create the ability to associate a problem in the *Test Case Daily Action Report* to an ITAMS ticket that might have additional information on the same problem. The *Test Case Daily Action Report* for the July 2011 disaster recovery test contained references to some of the ITAMS tickets that had been prepared. During the May 2011 disaster recovery test, participants were reminded that if a run or job in a test case has a problem, the related ITAMS ticket number should be included in the *Test Case Daily Action Report*. Therefore, it appears that the need to put ITAMS ticket numbers on the *Test Case Daily Action Report* has been at least anecdotally recognized.

If ITAMS tickets are not created and problem reporting is not improved, the risk increases that disaster recovery problems might not be properly identified, resolved, and tracked. In addition, disaster recovery test planners will have less information to review when they begin planning for the next disaster recovery test.

**Report recommendations to address some disaster recovery test problems are not closely or formally monitored**

Treasury Directive Publication 85-01, *Treasury Information Technology Security Program*, requires that bureaus have a process to track information technology security weaknesses and actions to correct them. Internal Revenue Manual 10.8.60, *Information Technology Security, Information Technology Disaster Recovery Policy and Guidance*,<sup>8</sup> requires that the IRS track and document findings and lessons learned and ensure that corrective action plans are implemented and findings are resolved.

The Cybersecurity organization does not closely or formally track the completion of all of the recommendations it makes in disaster recovery test *Executive Overview Reports*. The most serious recommendations are entered into the Plan of Action and Milestones tracking system, but less serious recommendations are not entered into a tracking system. Many of the recommendations in the *Executive Overview Reports* are not Plan of Action and Milestone type recommendations. Weekly meetings are held between Enterprise Operations and Cybersecurity organization staff, at which time they can discuss the recommendations and long-term issues/problems.

---

<sup>8</sup> IRM 10.8.60 (Jun. 1, 2009).



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

The Cybersecurity organization does not have a template for tracking the completion of some disaster recovery test corrective actions nor a matching standardized process to ensure that tracking is implemented continuously and on a repeatable basis.

When all disaster recovery test recommendations are not formally tracked, the risk increases that corrective actions may not be adequately addressed. Without a formal tracking template and process, the resources, time periods, and current status of the corrective actions might not be adequately defined and accomplished.

**Management Action:** During the course of the audit, we informed Cybersecurity organization staff of the need for an additional worksheet for tracking corrective actions. Cybersecurity staff developed a worksheet for this purpose, provided the worksheet to us for our review, and made modifications based on our suggestions. The worksheet was also vetted at a weekly disaster recovery test collaboration meeting, and the Cybersecurity organization staff plans to populate the worksheet with past test recommendations and update it during weekly meetings.

## ***Recommendations***

**Recommendation 1:** The Associate Chief Information Officer, Cybersecurity, should revise the *Test Case Daily Action Report* template to include an ITAMS/KISAM ticket column that would require the entry of the ITAMS/KISAM number for all problems reported on the *Test Case Daily Action Report* or a reason why an ITAMS/KISAM ticket is not required.

**Management's Response:** The IRS agreed with our recommendation. The IRS revised the *Test Case Daily Action Report* to include columns indicating run interruption, ITAMS/KISAM ticket number, and a reason why an ITAMS/KISAM ticket is not required.

**Recommendation 2:** The Associate Chief Information Officer, Cybersecurity, should create a process for reviewing the completeness of ITAMS/KISAM tickets and *Test Case Daily Action Reports* immediately after the disaster recovery test is completed so that the test staff can provide any missing information before reporting back to their regular duties.

**Management's Response:** The IRS agreed with our recommendation. The IRS developed a process for reviewing the completeness of ITAMS/KISAM tickets and *Test Case Daily Action Reports*.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

## Appendix I

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to observe IRS disaster recovery testing to determine whether the IRS is adequately testing its capability to recover major computer systems from one Computing Center<sup>1</sup> to another and whether systems can be successfully recovered. To accomplish our objective, we:

- I. Obtained and reviewed guidance and criteria on disaster recovery testing.
- II. Determined if the IRS adequately planned the July, August, and October 2011 disaster recovery tests.
  - A. Obtained and became familiar with the IRS *Disaster Recovery Test Plan*.
  - B. Determined if the *Disaster Recovery Test Plan* was adequately completed and that planned test cases were properly created in the *Test Case Daily Action Reports*.
  - C. Determined which computers and storage at the recovery site were used in the recovery test to ensure that disaster recovery testing was conducted in as close to an operational environment as possible.
  - D. Obtained and reviewed disaster recovery planning documents for the CADE 2.
- III. Observed the August and October 2011 disaster recovery tests to review disaster recovery testing procedures.
  - A. Observed during testing whether the *Disaster Recovery Test Plan* and planned test cases were followed and whether ITAMS tickets were prepared for problems encountered in performing the test cases.
  - B. Determined if any part of the *Disaster Recovery Test Plan* or planned test cases were not tested as planned based on observations, meeting attendance, and reports issued after the test.
  - C. Observed whether various disaster recovery testing procedures, instructions, and requirements were followed.

---

<sup>1</sup> See Appendix IV for a glossary of terms.



---

*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

- IV. Observed disaster recovery tests and reviewed disaster recovery testing reports for the July and August 2011 disaster recovery tests to determine if systems were successfully recovered.
  - A. Determined if recovered systems were tested to the point that users could use the system, jobs could be run, and other systems could exchange data with them.
  - B. Determined if any systems were recovered but not within stated recovery time objectives.
  - C. Determined if any systems were recovered but with problems (other than not meeting recovery time objectives).
  - D. Determined if any systems were not completely recovered and why.
- V. Reviewed IRS reports on the results of disaster recovery testing for the July and August 2011 disaster recovery tests.
  - A. Determined if a debriefing was held at the end of the disaster recovery test.
  - B. Obtained and reviewed IRS reports for evaluating test results and identifying weaknesses and corrective actions to improve IRS preparedness. These reports included the *Test Case Daily Action Report*, *Detailed Daily Observation Report*, *Vulnerabilities Matrix*, and *Executive Overview Report*.
  - C. Determined if the reports appeared to cover all the key issues or problems that we learned of during our observations of the test, attendance at meetings, or otherwise reported in disaster recovery reporting documentation.
  - D. Determined the IRS managers and executives who these reports were presented to.

**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 the following internal controls were relevant to our audit objective: the Cybersecurity organization's policies, procedures, and practices for planning, conducting, and reporting on disaster recovery tests. We evaluated these controls by interviewing staff of the Cybersecurity organization, observing disaster recovery tests, and reviewing plans and reports the IRS prepared on its disaster recovery tests.



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

**Appendix II**

*Major Contributors to This Report*

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Danny Verneuille, Director  
Carol Taylor, Audit Manager  
Myron Gulley, Acting Audit Manager  
Richard Borst, Senior Auditor  
Chinita Coates, Auditor  
Anthony Morrison, Program Analyst



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Deputy Chief Information Officer for Operations OS:CTO  
Associate Chief Information Officer, Applications Development OS:CTO:AD  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO  
Associate Chief Information Officer, Modernization Program Management Office OS:CTO:MP  
Director, Security Risk Management OS:CTO:C:SRM  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaison: Director, Risk Management Division OS:CTO:SP:RM



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

**Appendix IV**

*Glossary of Terms*

<b>Term</b>	<b>Definition</b>
Batch Processing	The execution of a series of programs or jobs on a computer with minimal human interaction.
Computing Center	IRS sites that support tax processing and information management through a data processing and telecommunications infrastructure.
Customer Account Data Engine 2	The next step in the IRS's information technology modernization efforts. The CADE 2 will provide faster refunds for millions of individual taxpayers and faster payment postings, account updates, and taxpayer notices. The CADE 2 will be implemented in a phased approach.
Cybersecurity Organization	Manages the IRS's Information Technology Security program. It is responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing measures to assure the confidentiality, integrity, and availability of IRS electronic systems, services, and data. It is within the Modernization and Information Technology Services organization.
Enterprise Life Cycle, Milestone 4B	A structured business system development method that requires the preparation of specific work products during different phases of the development process. Enterprise Life Cycle Milestone 4B is the completion of the System Development Phase, which is the first phase after the Design Phase. After Milestone 4B, the System Deployment Phase begins.
Enterprise Operations Organization	Provides server and mainframe computing services for all IRS business entities and taxpayers.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Fiscal Year	A 12-consecutive-month period ending on the last day of any month, except December. The Federal Government's fiscal year begins on October 1 and ends on September 30.



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

<b>Term</b>	<b>Definition</b>
Functional Exercises	Exercises in which recovery personnel execute their roles in a simulated operational environment. Functional exercises involve retrieving, loading, and validating backup tapes and files.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
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	The office within the Executive Office of the President that helps executive departments and agencies implement the commitments and priorities of the President.
Plan of Action and Milestones	A management process that outlines security weaknesses pertaining to a specific system and the steps that need to be taken to remediate them. It details resources required to accomplish the milestones in meeting the task and scheduled completion dates for the mitigation.
Recovery Time Objective	The maximum amount of time a system can remain unavailable before there is an unacceptable impact on other systems or supported business processes.
Table Top Exercises	Exercises that are discussion based and take place in a classroom setting. Participants use disaster recovery plans to discuss how they would respond to a disruption scenario.



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

**Appendix V**

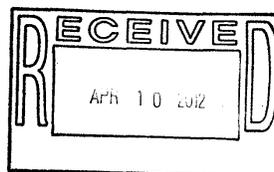
*Management's Response to the Draft Report*



CHIEF TECHNOLOGY OFFICER

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

APR 10 2012



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland *Terence V. Milholland*  
Chief Technology Officer

SUBJECT: Draft Audit Report – Disaster Recovery Testing Is  
Being Adequately Performed, but Problem Reporting  
And Tracking Can Be Improved  
(Audit # 201120024) (e-trak #2012-30307)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. We appreciate your report recognizing that the Internal Revenue Service is adequately planning and conducting disaster recovery tests of critical current production environment computer systems, as well as acknowledging the success of disaster recovery exercises and tests being performed on the Customer Account Data Engine 2 system as it is being developed. The test results confirmed the ability to replicate production data from the Martinsburg Computing Center to the Memphis Computing Center recovery site.

The IRS is committed to continuously improving the security of our information technology systems and disaster recovery processes. Your report recommendations will further improve our security posture. We agree with both of the report recommendations made as a result of your audit. The attachment to this memo details our planned corrective actions to implement the recommendations.

Your continued support and the assistance and guidance your team provides is a valuable resource to our organization. If you have any questions, please contact me at (202) 622-6800 or David Stender, Associate Chief Information Officer for Cybersecurity, at (202) 622-8910.

Attachment



*Disaster Recovery Testing Is Being Adequately Performed,  
but Problem Reporting and Tracking Can Be Improved*

Attachment

Draft Audit Report – Disaster Recovery Testing Is Being Adequately Performed, but Problem Reporting and Tracking Can Be Improved (Audit # 201220024) (e-trak #2012-30307)

**RECOMMENDATION #1:** The Associate Chief Information Officer, Cybersecurity, should revise the *Test Case Daily Action Report* template to include an ITAMS/KISAM ticket column that would require the entry of the ITAMS/KISAM number for all problems reported on the *Test Case Daily Action Report* or a reason why an ITAMS/KISAM ticket is not required.

**CORRECTIVE ACTION #1:** The IRS agrees with the recommendation and has made the necessary changes to the Test Case Daily Action Report to include 3 revised columns indicating Run Interruption, KISAM Ticket Number, and Explanation (if a ticket is not opened). The changes were made to both the Martinsburg (MTB) to Memphis (MEM) Test Case Daily Action Report template and to the Memphis to Martinsburg template.

**IMPLEMENTATION DATE:** Completed

**RESPONSIBLE OFFICIAL:** ACIO, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES).

**RECOMMENDATION #2:** The Associate Chief Information Officer, Cybersecurity, should create a process for reviewing the completeness of ITAMS/KISAM tickets and Test Case Daily Action Reports immediately after the disaster recovery test is completed so that the test staff can provide any missing information before reporting back to their regular duties.

**CORRECTIVE ACTION #2:** IRS agrees with recommendation and has made the necessary changes to the DR Test Plan template to “create a process for reviewing the completeness of ITAMS/KISAM tickets and Test Case Daily Action Reports” as recommended. The modifications made to the DR Test Plan, Part A, entitled DR Test General Information, are as follows:

- Add item 9.(a) KISAM Problem Reporting - Status Meetings, and
- Revise item 11, Populate Test Case Daily Action Report, to include the sentence “Ensure that KISAM ticket numbers are entered in the appropriate column as problems are reported via KISAM during the DR Test recovery/restoration.”

**IMPLEMENTATION DATE:** Completed

**RESPONSIBLE OFFICIAL:** ACIO, Cybersecurity

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES).