



*Customer Account Data Engine 2 (CADE 2):  
System Requirements and Testing  
Processes Need Improvements*

**September 28, 2012**

**Reference Number: 2012-20-122**

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

### **CUSTOMER ACCOUNT DATA ENGINE 2 (CADE 2): SYSTEM REQUIREMENTS AND TESTING PROCESSES NEED IMPROVEMENTS**

## Highlights

**Final Report issued on  
September 28, 2012**

Highlights of Reference Number: 2012-20-122 to the Internal Revenue Service Chief Technology Officer.

### **IMPACT ON TAXPAYERS**

The implementation of Customer Account Data Engine 2 (CADE 2) daily processing allows the IRS to process tax returns for individual taxpayers more quickly by replacing existing weekly processing. The CADE 2 system also provides a centralized database of individual taxpayer accounts, allowing IRS employees to view tax data online and provide timely responses to taxpayers. The successful implementation of the CADE 2 system should significantly improve service to taxpayers and enhance IRS tax administration.

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

The overall objective was to determine whether the CADE 2 Transition State 1 testing activities were performed in accordance with applicable policies and procedures.

### **WHAT TIGTA FOUND**

The IRS initiated testing of the CADE 2 system, reduced the risks to the filing season by implementing independent contractor recommendations, and performed simulated exercises to identify potential issues that could occur during the filing season. Improvements are needed in key controls and processes for requirements management, testing processes, and developer security testing.

### **WHAT TIGTA RECOMMENDED**

TIGTA recommended that the Chief Technology Officer ensure test cases and other appropriate documentation are properly developed for

infrastructure requirements; all infrastructure documentation includes complete traceability to the requirements being tested and the testing results; IRS testers obtain and maintain documentation to verify test results; test execution practices are consistent; all security requirements and corresponding test cases are identified and sufficiently traced, managed, and tested; all database issues identified by Vulnerability Detection Scans are resolved or an action plan is developed with specific corrective actions and time periods; and all issues identified by Source Code Security Review scans are resolved and an action plan is developed with specific corrective actions prior to the code being placed into service.

In management's response to the report, the IRS disagreed or partially disagreed with three of our eight recommendations. The IRS disagreed with developing an enterprise-wide program level Requirements Traceability Verification Matrix (RTVM) and policy. TIGTA believes an enterprise-wide approach is needed to strengthen oversight of traceability controls.

The IRS also disagreed with the recommendation that RTVMs are prepared during the test Initiation Phase. However, as discussed with CADE 2 officials, our report refers to both Requirements Traceability Matrix and RTVM as "RTVM."

Further, the IRS stated that automated tools are not always needed for control of requirements and test case management for Information Technology systems development. TIGTA maintains that use of one suite of integrated automated tools would provide needed control over volumes of requirements and test cases for IRS systems, including the monumental CADE 2 system development program.

Lastly, the IRS stated that additional CADE 2 documentation is not needed to ensure complete traceability of requirements to test results. The IRS believes that adequate documentation already exists with Government Equipment Lists and environmental checklists. However, while this documentation does verify that infrastructure components have been acquired and implemented, it does not verify that all CADE 2 processing requirements have been tested.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 28, 2012]

**MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER**

**FROM:** Michael E. McKenney  
Acting Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – Customer Account Data Engine 2 (CADE 2):  
System Requirements and Testing Processes Need Improvements  
(Audit # 201120005)

This report presents the results of our review of the Customer Account Data Engine 2 Transition State 1 testing activities. Our overall objective was to determine whether testing activities were performed in accordance with applicable policies and procedures. This review was requested by the Chief Technology Officer and was included in our Fiscal Year 2011 Annual Audit Plan. This review addresses the major management challenge of Modernization of the Internal Revenue Service.

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

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



---

*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

## *Table of Contents*

<b>Background</b> .....	Page 1
<b>Results of Review</b> .....	Page 3
The Internal Revenue Service Performed Extensive Testing, Planned Risk Reduction, and Implemented Controls Over CADE 2 Transition State 1 System Development.....	Page 3
Requirements Management Controls Need Improvement to Ensure Long-Term Success of the CADE 2 Program .....	Page 5
<u>Recommendation 1:</u> .....	Page 7
<u>Recommendation 2:</u> .....	Page 8
Test Management Controls Need Improvement to Ensure Long-Term Success of the CADE 2 Program.....	Page 8
<u>Recommendations 3 through 5:</u> .....	Page 15
Identified Security Issues Need to Be Resolved.....	Page 16
<u>Recommendations 6 through 8:</u> .....	Page 20
<b>Appendices</b>	
Appendix I – Detailed Objective, Scope, and Methodology .....	Page 21
Appendix II – Major Contributors to This Report.....	Page 23
Appendix III – Report Distribution List .....	Page 24
Appendix IV – Glossary of Terms.....	Page 25
Appendix V – Management’s Response to the Draft Report .....	Page 31



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

## *Abbreviations*

CADE 2	Customer Account Data Engine 2
DI	Database Implementation
DP	Daily Processing
FIPS	Federal Information Processing Standards
IMF	Individual Master File
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST SP	National Institute of Standards and Technology Special Publication
PMO	Program Management Office
ReqPro	Rational Requisite Pro
RTVM	Requirements Traceability Verification Matrix
TS1	Transition State 1



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

### *Background*

In January 2010, the Internal Revenue Service (IRS) Commissioner signed the Program Charter authorizing the formation of the Customer Account Data Engine<sup>1</sup> 2 (CADE 2) Program to build on the substantial progress the current CADE processing platform had accomplished and to leverage lessons learned to date. The IRS

Information Technology organization<sup>2</sup> has a lead role in developing and implementing the CADE 2 system. The CADE 2 Program was also created to address the risks of the current CADE approach and to implement fundamental changes to the core IRS

***The CADE 2 Program is critical to the IRS's mission and its most important information technology investment.***

business systems. The CADE 2 Program should achieve defined goals and manage and integrate all the required components such as enhancement projects, new and legacy applications, business processes, organizational changes, and policy and procedure modifications.

The CADE 2 Program Management Office's (PMO) approach for delivery of the CADE 2 Program is a functional and technical progression through two transition states to a target state. Transition State 1 (TS1) has two main purposes: 1) the Database Implementation (DI) project is intended to establish a relational database that will house all individual taxpayer accounts and provide the ability for IRS employees to view the updated account information online and 2) the Daily Processing (DP) project is intended to provide individual taxpayer account information to select external systems on a daily basis as opposed to the current weekly basis. The IRS implemented the daily processing portion of TS1 in January 2012. The database portion of TS1 will follow daily processing. Transition State 2 is expected to address financial material weaknesses and build or modify existing applications to directly interact with the CADE 2 database. The target state for the CADE 2 system entails completing the transition of all planned Information Technology applications and realizing the business benefits expected with the system.

Within the IRS Information Technology organization, the Application Development Enterprise Systems Testing organization, in partnership with the CADE 2 PMO, is responsible for planning and executing the testing activities required for verifying and validating the overall TS1 solution. The Enterprise Systems Testing CADE 2 Testing Integration Office was established expressly to support the CADE 2 Program and is responsible for planning, scheduling, coordinating, and reporting on all CADE 2 system testing activities. CADE 2 testing processes are coordinated at

---

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

<sup>2</sup> As of July 1, 2012, the Modernization and Information Technology Services organization officially changed its name to the IRS Information Technology organization.



## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

the program level, and the TS1 comprehensive test schedule is maintained in the Individual Master File (IMF) Schedule. The Cybersecurity organization is an Enterprise Systems Testing organization test service partner<sup>3</sup> responsible for conducting security testing activities designed to ensure the system's security safeguards are in place and functioning as intended.

This review was requested by the Chief Technology Officer and was performed at the IRS Information Technology organization facilities in New Carrollton, Maryland; Memphis, Tennessee; and Martinsburg, West Virginia, during the period June 2011 through June 2012. During audit fieldwork, we concurrently advised CADE 2 testing officials when issues were identified and suggested corrective actions. We also communicated preliminary audit results and recommendations for improvement to the Associate Chief Information Officer for Modernization – Program Management Office on October 7, 2011, December 12, 2011, and February 16, 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>3</sup> A test service partner is an organization external to the Enterprise Systems Testing organization that performs tests for the CADE 2 Program, through a test brokering agreement.



---

*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

*Results of Review*

***The Internal Revenue Service Performed Extensive Testing, Planned Risk Reduction, and Implemented Controls Over CADE 2 Transition State 1 System Development***

The Department of the Treasury procedures for information technology strategic planning and portfolio management require bureaus to establish and maintain development processes and procedures to ensure effective planning and execution of development activities and use of a standardized systems development life cycle methodology. The IRS relies on its Enterprise Life Cycle methodology to guide systems development activities, which include system testing. Our review of CADE 2 TS1 testing activities considered the performance of extensive testing, independent assessments from two contractors, performance of simulation exercises, and improved controls to reduce risk and ensure the success of the CADE 2 system.

***The IRS performed extensive testing of CADE 2 TS1***

The IRS performed several types of testing, including the Accessibility Test,<sup>4</sup> User Acceptance Test, Systems Acceptance Test, Final Integration Test Phase 1, Final Integration Test Phase 2 (2012 Filing Season), Developer Security Testing, Source Code Security Review, and Vulnerability Detection Scans prior to the implementation of daily processing in January 2012. The IRS implemented Final Integration Test Phase 1 as an additional testing process to decrease the risks of adverse impact on the 2012 Filing Season. The purpose of Final Integration Test Phase 1 was to demonstrate that the CADE 2 programs would work correctly in a near-production environment. Final Integration Test Phase 1 also allowed IRS executives sufficient time to make any necessary contingency decisions.

***Independent contractor assessments identified risks and concerns***

The IRS contracted with two consulting firms to perform independent assessments of the CADE 2 system to identify concerns and areas of risk that needed mitigation. One of the contractor's assessments determined that the Systems Acceptance Test was behind schedule, continued to experience delays, and reported that less than one-half of the test routines were executed. This resulted in the IRS adding test resources and extending the timelines for Systems Acceptance Test delivery to December 30, 2011. Additionally, the assessment determined that

---

<sup>4</sup> Accessibility Testing is required by Federal agencies to maintain a technical environment that is accessible to employees with disabilities and to the public at large. As a Federal agency, the IRS must ensure all information content and systems comply with mandated technical and functional performance criteria.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

operational testing did not support the IRS's ability to handle a full weekly cycle in the allotted time. The IRS responded by reviewing cycle times during an early January 2012 tax processing run. By implementing specific recommendations from the contractor assessments, the IRS reduced filing season risks. With this action, the IRS was able to utilize the independent assessment reports to take necessary steps toward developing confidence and ensuring readiness for the TS1 deployment in January 2012.

### **The IRS performed simulated exercises to identify potential issues that could occur during the 2012 Filing Season**

The IRS conducted CADE 2 processing simulation exercises to identify and correct potential business processing issues. Tabletop exercises validated the processes and procedures that would be executed for TS1 during the 2012 Filing Season. We observed five tabletop exercises and determined that the IRS identified potential CADE 2 processing problems and developed action items to address these concerns.

For example, one tabletop session looked at IMF processing in which the participants learned to identify and correct any potential tax processing issues prior to the January 2012 implementation of the CADE 2 DP project application. In one scenario for which a typical computer file was not received during the processing day, the participant learned how to correct the problem within the same day and still complete the processing. After tabletop sessions, action items are reviewed, validated, and assigned during session debriefs. The IRS also subsequently tracks the status of the action items to ensure completion.

### **The IRS implemented controls over the CADE 2 Program**

The Chief Technology Officer also implemented corrective actions to address our prior audit<sup>5</sup> recommendations. Controls were implemented to help prevent CADE 2 Program stakeholders from removing and working on CADE 2 customer requirements outside of the Rational Requisite Pro (ReqPro) application and to help them use this tool to fully manage the creation and revisions of requirements. To accomplish this, the IRS provided training on ReqPro, held monthly user group training sessions on advanced ReqPro topics, and ensured that the CADE 2 requirements were input into ReqPro.

The IRS also ensured requirements were managed in ReqPro prior to test execution. To accomplish this, the CADE 2 PMO held weekly Integrated Requirements Team meetings with all delivery partners to identify and mitigate requirement gaps and to help ensure requirements were traced within ReqPro. The benefits of these corrective actions were intended to help ensure ReqPro is utilized appropriately to manage CADE 2 requirements.

---

<sup>5</sup> Treasury Inspector General for Tax Administration, Ref. No. 2011-20-127, *Customer Account Data Engine 2 Program Management Office Implemented Systems Development Guidelines; However, Process Improvements Are Needed to Address Inconsistencies* (Sept. 2011).



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

### **Requirements Management Controls Need Improvement to Ensure Long-Term Success of the CADE 2 Program**

Requirements are used to define specific business and technical functionalities that are needed from a system. Traceability is a key component of requirements management and involves the ability to describe and trace the life of a requirement from its source and through the complete testing life cycle, in both a forward and backward direction. The CADE 2 Requirements Management Plan and Internal Revenue Manual (IRM) 2.6.1, *Product Assurance – Test, Assurance & Documentation Standards and Procedures*, provide guidelines for development of requirements and tracing those requirements to their sources and to test cases. IRM 2.6.1 also defines the testing life cycle and details when a Requirements Traceability Verification Matrix (RTVM) is to be developed in relation to when test cases are to be developed and executed. The RTVM and test cases should be developed before initiation of testing activities, and the matrix should be updated and accurately maintained throughout the requirements management and testing processes.

The ReqPro automated tool is the standard, within the IRS Enterprise Architecture, for requirements management. All CADE 2 Program, project, and stakeholder personnel should use ReqPro to create, manage, and control requirements and to maintain traceability across the Program and projects. ReqPro can generate an RTVM to record and track requirements.

The CADE 2 PMO established a ReqPro repository to manage and baseline all CADE 2 requirements. However, the CADE 2 PMO did not develop and deliver a program-level RTVM prior to initiating testing activities to ensure the Enterprise Systems Testing organization subsequently traced the CADE 2 requirements to test cases and test case results. Instead, the CADE 2 PMO first allocated the requirements to the Applications Development organization. Subsequently, the Applications Development organization mapped the requirements to the Unified Work Request document and allocated these requirements to the appropriate teams. The requirements were then decomposed into specific CADE 2 requirements.

According to discussions and documentation provided by the IRS, the Applications Development organization teams developed approximately 40 project-level RTVMs with these requirement details and delivered the requirements via the RTVMs to the Enterprise Systems Testing organization and the CADE 2 testing partners. The Enterprise Systems Testing organization and the CADE 2 testing partners did adhere to the IRS standard of tracing CADE 2 requirements to test cases in the RTVMs, and they further developed these RTVMs by adding test data such as test cases and test results.

The CADE 2 PMO was responsible for verifying the Enterprise System Testing organization's traceability work. Therefore, the Enterprise System Testing organization delivered the final RTVMs to the CADE 2 PMO. The CADE 2 PMO relied on a manual, ad hoc process to verify whether CADE 2 requirements had been traced to test cases by the Enterprise Systems Testing organization. However, we found that the CADE 2 PMO did not complete this verification



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

process prior to the implementation of the CADE 2 DP project in January 2012. According to the CADE 2 Requirements Measures and Metrics report dated January 17, 2012, there are a total of 2,317 approved CADE 2 TS1 customer requirements, of which 468 (20 percent) requirements were specifically related to the DP project. According to this same report, when the DP project was implemented in January 2012, the CADE 2 PMO had only verified 53 (11 percent) of the 468 DP specific requirements through its manual, ad hoc process.

The CADE 2 PMO did not complete this verification process prior to the implementation of the DP project because of numerous associated issues with the RTVMs provided by the Enterprise Systems Testing organization. For example, CADE 2 RTVMs were grouped with others that were not related to the CADE 2 Program. This necessitated that the PMO complete a difficult process to determine which RTVMs were related to the CADE 2. Further, after the PMO ascertained which RTVMs were related to the CADE 2, it was determined that the CADE 2 RTVMs themselves also included other requirements and test cases that were not related to the CADE 2 Program. To address this challenge, the PMO then initiated another difficult process to delineate the CADE 2-related requirements and test cases needed. As a result, the IRS did not have sufficient assurance that all approved customer requirements were included in test cases and tested prior to the implementation of the DP project in January 2012.

In addition, the process to ensure all requirements were traced to test cases was complicated by use of new tools for requirements management and test case management. This included ReqPro for managing all CADE 2 requirements and Rational Quality Manager for developing and managing a portion of the CADE 2 test cases. Control over CADE 2 requirements and test cases was also complicated because one suite of interacting automated tools was not being fully used to develop, manage, and bidirectionally trace requirements and test cases or to monitor, manage, and bidirectionally trace test case defects with test cases and requirements. The CADE 2 PMO and CADE 2 testing partners are using a mixture of manual processes and automated tools that do not interact and bidirectionally trace in an automated fashion.

Without program-level traceability between the thousands of CADE 2 requirements and test cases, the IRS faces increased risks that some requirements may not be included in test cases and be tested. As a result, the possible impact of incomplete, missing, or invalid requirements could have an adverse impact on CADE 2 functionality and successful implementation in the long term. Further, implementing this important management control would help to ensure taxpayer's trust in this IRS system.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

### **Recommendations**

The Chief Technology Officer should ensure:

#### **Recommendation 1:**

- a. Requirements and corresponding test cases are identified and sufficiently traced, managed, and tested prior to the CADE 2 DI project implementation to ensure the CADE 2 system operates as intended.
- b. Enhanced oversight of traceability controls are implemented enterprise-wide. This includes developing a program-level RTVM prior to the test Initiation Phase of IRM 2.6.1 and updating that program-level RTVM to include test cases and final tests results. This process should be formally documented.
- c. The CADE 2 PMO provides enhanced oversight of the traceability controls. This includes developing and providing a program-level RTVM prior to the test Initiation Phase of IRM 2.6.1, and that the program-level RTVM is updated to include test cases and final tests results. This process should be formally documented.

**Management's Response:** The IRS agreed with Recommendation 1a. The IRS stated it will ensure that CADE 2 requirements and corresponding test cases are identified and sufficiently traced, managed, and tested prior to the CADE 2 Database Implementation.

However, the IRS disagreed with Recommendations 1b and 1c. The IRS stated it has not committed to enterprise-wide program-level RTVMs or program-level testing IRMs for using program RTVMs. The IRS agreed with the principle of program-level traceability, but it does not agree that it needs to be implemented through an RTVM artifact, and that it has already complied with Recommendation 1c with the development of a CADE 2 Program RTVM. The IRS also disagreed with the two recommendations based on what it believes to be inaccuracies in the content of the recommendations, in that the RTVMs are prepared during the test Initiation Phase, not before the test Initiation Phase.

**Office of Audit Comment:** We maintain an enterprise-wide RTVM and policy are necessary to strengthen oversight of traceability controls for the CADE 2. Also, the IRS states RTVMs are prepared during the test Initiation Phase, not before. However, as stated in the report, we refer to the Requirements Traceability Matrix and RTVM as the "RTVM" for clarification purposes. The program-level RTVM should be maintained throughout the requirements management and testing processes to ensure complete functionality and long-term successful implementation for the CADE 2 system.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

### **Recommendation 2:**

- a. A standard suite of integrated, automated tools is implemented enterprise-wide to enable programs and projects to develop and manage requirements, develop and manage test cases, bidirectionally trace requirements and test cases, monitor and manage test case defects, and bidirectionally trace test case defects with test cases and requirements.
- b. A standard suite of integrated, automated tools is implemented for CADE 2 Transition State 2 and all future CADE 2 projects to develop and manage requirements, develop and manage test cases, bidirectionally trace requirements and test cases, monitor and manage test case defects, and bidirectionally trace test case defects with test cases and requirements.

**Management's Response:** The IRS disagreed with Recommendations 2a and 2b. The IRS stated it has not committed to a policy, or funded a project, to standardize and implement tools on an enterprise-wide level, and that neither recommendation offers any flexibility for projects that are not good candidates for automated tools. Automated tools are not always necessary to maintain control over requirements and test case management, traceability, *etc.*, so the IRS does not agree with our prescribing their use.

**Office of Audit Comment:** As discussed with CADE 2 officials during the audit closing conference, it is important that this recommendation be fully addressed and we delineated the recommendation into two parts for clarification on the weaknesses contributing to our finding and also for tracking purposes. We maintain that a suite of integrated automated tools is needed to ensure that all requirements are included in test cases and appropriately tested for the CADE 2 system. Recommendation 2a addresses the need for the IRS to establish an enterprise approach to system requirements, including integrated, automated testing tools. Recommendation 2b addresses the need for such integrated, automated tools to support all phases of the CADE 2 system and to better ensure long-term success for this ground breaking mission critical system.

### **Test Management Controls Need Improvement to Ensure Long-Term Success of the CADE 2 Program**

The IRS implemented the CADE 2 testing processes to validate that the TS1 solution would function as designed and meet the IRS's tax processing objectives once the system is implemented during the 2012 Filing Season. Adequate testing helps ensure that costly retrofits are avoided after a system is implemented. According to IRS guidelines, CADE 2 requirements must be reviewed and accepted before they are approved for testing. We judgmentally<sup>6</sup> reviewed 49 of 3,083 approved system requirements and 48 of 1,530 unapproved system requirements as

---

<sup>6</sup> A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

of September 1, 2011. The 48 unapproved requirements were deferred, proposed, rejected, or transferred.<sup>7</sup> Our review of requirements testing activities identified several test management concerns that could affect the success of the CADE 2 Program.

### **Documenting test cases and test results**

IRM 2.6.1 provides guidelines for testing and is used as a guide to develop detailed test plans for the CADE 2 system. The IRM states that test cases should be developed to support requirements testing, and IRS testers should obtain and maintain evidence of the actual test results. The test cases should include the requirements being tested, expected results, and documentation of whether the requirements passed or failed during test execution. The tester should also maintain evidence to validate the actual test results, which could include computer screen prints, input and output data files, and system logs. During the test execution phase, test results should be reviewed and validated.

In 12 (24 percent) of the 49 approved requirements that we reviewed, the IRS did not ensure test cases were developed. Also, in 14 (29 percent) of the 49 approved requirements we reviewed, the IRS could not always provide objective evidence the requirements were sufficiently tested prior to the deployment of CADE 2 TS1 in January 2012.

Developing test cases for the infrastructure requirements – The 12 requirements sampled which did not have test cases were infrastructure requirements. IRS management advised us that there are two types of infrastructure requirements affecting the CADE 2 system:

- Process Automation and Monitoring Requirements – requirements that deal with the scheduling and monitoring of CADE 2 Programs.
- Environmental Design Requirements – requirements that deal with the creation of environments in which to develop, test, and implement final CADE 2 systems and business functionality.

---

<sup>7</sup> The requirement populations mentioned here do not include performance and capacity requirements, which were reviewed in the Treasury Inspector General for Tax Administration, Ref. No. 2012-20-051, *Customer Account Data Engine 2 Performance and Capacity Is Sufficient, but Actions Are Needed to Improve Testing* (May 2012).



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Figure 1 provides examples of specific infrastructure requirements that did not have a test case.

**Figure 1: Infrastructure Requirements That Did Not Have a Test Case**

Abbreviated Requirement Description	Test Type and Project
The Monitoring Agent/Probe shall systematically capture “Time Finish” for batch process...in standardized machine readable format.	Processing Automation and Monitoring Infrastructure/DP
The Correlation Engine shall systematically forward alerts when “Out of Balance” is determined to be in...IMF Pre-Cutoff Processing.	Processing Automation and Monitoring Infrastructure/DP
The Monitoring Agent/Probe shall systematically capture “Time Start” for batch process...in standardized machine readable format.	Processing Automation and Monitoring Infrastructure/DP
Infrastructure shall provide capability for the IMF to send Revenue Accounting Control System Data to Redesign Revenue Accounting Control System on a daily basis.	Environmental Design Infrastructure/DP
The system shall support automated and manual configuration of setup and workflow information.	Environmental Design Infrastructure/DI
The system should rely primarily on existing platforms, communications, and technologies already operating within the enterprise.	Environmental Design Infrastructure/DI and DP
Infrastructure shall provide capability for the IMF to send TRANSCRIPT...to CADE 2 Transcripts-IMF on a daily basis.	Environmental Design Infrastructure/DP
The system shall provide storage management...mainframe platform.	Environmental Design Infrastructure/DP
The system shall have development environments.	Environmental Design Infrastructure/DI

*Source: CADE 2 ReqPro extract as of September 1, 2011, and information from the IRS related to the selected requirements samples.*

There were four processing automation and monitoring requirements within our audit sample that did not have verifiable test cases. We were unable to determine whether these were the correct test cases because the unique processing automation and monitoring requirement numbers were not included in the test cases, nor were the specific IRS processing runs included in the requirements. Instead, the test cases included other processing runs, and the IRS testers recorded that those processing runs passed during test execution. Therefore, we were unable to verify these were the correct test cases for testing the requirements in question.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

The remaining eight requirements from our sample that did not have test cases were for environmental design requirements. IRS management stated that test cases were not applicable to these environmental design requirements because they are more appropriately validated through the use of various infrastructure documents. These documents include Government equipment lists developed to identify the hardware and software purchases needed to prepare the environments and environmental checklists used to provide evidence that the equipment has been installed and is ready for use. The IRS testing staff stated they purchased the equipment needed for the environments that would support the CADE 2 system, installed the equipment, and performed preliminary tests to ensure the equipment was ready for use to fulfill its processing requirements. However, the infrastructure documents, in some instances, do not trace back to the specific environmental design requirements they are intended to verify. Also, when the environmental design requirements included an IRS processing element, the infrastructure documents did not provide evidence that the processing capabilities, such as transmitting data daily between IRS systems, were tested prior to implementing the system.

During our review, the IRS did not believe that the methods it relied on to verify environmental design requirements were deficient. However, IRS officials acknowledged our concern, particularly with the environmental design requirements that have IRS processing features, and the IRS agreed to perform additional research on applicable guidelines for testing these types of systems development requirements. We believe that improved controls are needed in this area to ensure complete testing of the CADE 2 infrastructure and to avoid possible adverse effects on CADE 2 functionality.

Documenting evidence of test results – The IRS could not always provide actual test results evidence for the 14 requirements we reviewed. Additionally, five of these 14 requirements covered DP project activities that did not include an infrastructure requirement that was implemented in January 2012. The remaining nine were infrastructure requirements for processing automation and monitoring (five requirements) and environmental design (four requirements). The IRS did not provide any evidence to validate the five processing automation and monitoring requirements. The IRS did not ensure testers were following IRM guidelines to obtain and maintain objective evidence such as screen prints and input and output files to verify that requirements were sufficiently tested. As a result, there was not an adequate system in place to provide actual test results.

For the four environmental design requirements, we determined that the IRS provided valid evidence of test results when we could reasonably identify traceability of the requirements to design documentation, the equipment purchased, and ready-for-use checklists. However, when the environmental design requirements included IRS processing elements, the documentation provided by the IRS did not provide any evidence that the processing capabilities had been tested. For example, all four of the environmental design requirements contained some processing capabilities. However, the design documents, Government equipment lists, and ready-for-use checklists did not provide evidence that these requirements were tested.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

If the documents used to verify actual test results are not available, then the IRS cannot verify the adequacy of its systems testing activities. In addition, we could not verify the results of these requirements prior to the implementation of CADE 2 TS1 in January 2012.

IRS management acknowledged that testers should obtain evidence to validate actual test results in accordance with the IRM. After we presented this finding, the IRS initiated a review of IRM guidelines and identified inconsistencies in the procedures for obtaining evidence of actual test results. As a result, the IRS agreed that the IRM may need clarification in regards to obtaining evidence to validate actual test results.

**Management Action:** Following our audit fieldwork, the IRS provided us with some documentation for DP project test results.

**Determining the testability of requirements**

The CADE 2 Requirements Management Plan includes the guidelines for developing quality requirements, including ensuring the requirements are “specific enough to implement and test.” Our review identified that six (12 percent) of 49 sampled approved requirements could not be tested. The IRS did not ensure that quality review processes, like Customer Technical Reviews, effectively identified and addressed requirements that could not be tested. For example, requirements that could not be tested were: 1) written at a high-level; 2) not specific as written, but were deemed to be covered by many other requirements and test cases; 3) included to update operating procedures; and 4) a request from the IRS business unit to capture bad data from the IMF. Figure 2 describes requirements from our audit sample that could not be tested and the reasons provided by the IRS for not testing the requirements.

***Figure 2: Requirements That Could Not Be Tested***

Requirement Description	Project	Reason the Requirement Could Not Be Tested
The system shall flag data that are the incorrect classification for correction during the load if it is needed for tax/financial obligation.	DI	The requirement is not specific as written. This is a request from the business unit to capture unknown ‘bad’ data from the IMF. DI project development created tables and provided the captured data to the business unit for review. There is no test case required.
The system shall transform input data to the format required by the CADE 2 database.	DI	This requirement is not specific as written. The IRS stated testing for this requirement is covered by many other requirements, so there is no test case for this specific requirement identification number.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Requirement Description	Project	Reason the Requirement Could Not Be Tested
The system shall utilize the automated scheduling system to schedule transaction input files for processing daily.	DP	This requirement involves current processing and a test case is not required.
The system shall ensure that the Integrated Data Retrieval System synchronizes with the current processing cycle.	DP	This was not a true requirement that can be developed. It is a requirement to prompt coordination. The CADE 2 PMO has coordinated with all stakeholders to ensure that the Integrated Data Retrieval System and all other downstream systems are in sync with the current processing cycle.
The organization shall save all production test results for two years.	DP	This is a procedural requirement to have operating procedures updated to reflect the change. No associated test case is needed.
The system shall notify downstream systems of daily updates.	DP	This requirement could not be tested at this high level, and there is no test case associated. This would be covered under other specific requirements.

*Source: CADE 2 ReqPro extract as of September 1, 2011, and information from the IRS related to the selected requirement samples.*

During the audit, IRS management acknowledged the finding and agreed to take needed steps to clarify the IRM on the development of requirements. The inclusion of requirements that could not be tested could result in insufficiently developed test cases. When the IRS creates test cases for requirements that are not specific enough to test, the IRS does not have assurance that these test cases are appropriate. If the results from inappropriate test cases are accepted, they could adversely affect the operation of the CADE 2 system.

**Deferring requirements without following the change management process**

The CADE 2 Requirements Management Plan indicates that formal change documents should be prepared when a requirement is deferred, such as change requests and impact assessments. For the CADE 2 Program, change requests must be approved by the Change Control Board. Further, assessments are needed to identify the impact of deferred requirements on other requirements and system functionality. We identified 12 approved requirements and three proposed requirements which had been deferred outside of these change management guidelines. This included deferred requirements for forwarding alerts when outbound dollar values reach or exceed predetermined thresholds. Other deferred requirements related to capabilities to capture outbound transaction counts and inbound dollar values. The IRS did not ensure the required change requests and impact assessments were prepared prior to deferring these requirements.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

IRS staff advised us that it did not prepare formal documentation for these deferred requirements because the requirements were not deferred to another release (such as CADE 2 Transition State 2). Without following the established change management guidelines to include the preparation of impact assessments, users and stakeholders are unable to ascertain the potential impacts of the deferred requirements on other CADE 2 requirements and system functionality.

**Management Action:** The IRS acknowledged that the Requirements Management Plan requires the change management process be fully followed in making decisions to defer requirements. However, the CADE 2 requirement procedures specifically refer to requirements being deferred to a future release. The requirements being deferred in our finding were not deferred to a future release. IRS management stated, however, that our inquiry highlighted a gap in their process regarding deferral of requirements within a release. As a result, the IRS plans to expand its change management processes to include deferring and tracking requirements within a release. This action should ensure that all stakeholders have assessed the potential impacts.

### **Ensuring testers follow established guidelines during test execution**

We observed several IRS testers to ensure CADE 2 tests were successfully executed according to guidelines provided in IRM 2.6.1. These procedures require IRS testers to document the results, follow the test scripts, update the test cases during test execution, and maintain sufficient evidence so the results of testing can be verified during test execution. During 11 on-site test observations, testers: 1) did not always consider the most recent changes prior to executing a test case, 2) did not update the test script with observed changes until after the test was executed, 3) experienced a slow response and were unable to access Rational Quality Manager when ready to record tests results, and 4) did not always have access to the Rational Quality Manager reporting functionality. These conditions indicate that IRS management did not ensure its testers consistently followed required IRM guidelines. The risk of incomplete or invalid testing is increased when testers do not follow required test execution practices. Also, invalid testing could adversely affect CADE 2 functionality.

**Management Action:** IRS management stated that the Rational Quality Manager pilot team provided feedback showing that the Rational Quality Manager reporting function was performing adequately and availability and accessibility had been good. In addition, the reporting component of Rational Quality Manager was being implemented and configured at the same time as our audit fieldwork.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

### **Recommendations**

The Chief Technology Officer should ensure:

**Recommendation 3:** IRM guidelines are followed, specifically that:

- a. Test cases and other appropriate documentation are properly developed for infrastructure requirements and all infrastructure documentation includes complete traceability to the requirements being tested and the testing results.
- b. IRS testers obtain and maintain documentation to verify test results.
- c. Test execution practices are consistent prior to the CADE 2 DI project implementation.

**Management's Response:** The IRS agreed with Recommendations 3b and 3c. The IRS stated it will ensure that IRM guidelines are followed, that IRS testers obtain and maintain documentation to verify test results, and that test execution practices are consistent prior to CADE 2 DI project implementation.

However, the IRS disagreed with Recommendation 3a. The IRS believes that appropriate documentation already exists for infrastructure requirements with the association of Government Equipment Lists and environmental checklists that provide sufficient assurance that infrastructure components have been acquired and implemented.

**Office of Audit Comment:** While the IRS's documentation does verify that infrastructure components have been acquired and implemented, we maintain that additional infrastructure documentation is needed to verify that processing requirements have been tested and to better ensure complete CADE 2 functionality and successful long-term implementation of this critical system.

**Recommendation 4:** Quality review processes, including Customer Technical Reviews, identify, correct, or remove requirements that could not be tested prior to the implementation of testing activities.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated it will develop procedures to ensure that quality review processes identify, correct, or remove requirements that could not be tested prior to the implementation of testing activities, which will include Customer Technical Reviews.

**Recommendation 5:** Formal change management processes are implemented for all deferred and proposed requirements prior to the CADE 2 DI project implementation.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated it will develop procedures to ensure a formal change management process for all deferred and proposed requirements.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

### ***Identified Security Issues Need to Be Resolved***

The Security Assessment and Authorization process is designed to ensure that an information system will operate with the appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically. As part of this process, the Cybersecurity organization conducted a CADE 2 Security Control Assessment to ensure the CADE 2 system's security safeguards are in place and functioning as intended. The Security Control Assessment is an analysis of nontechnical and technical security controls required to protect information in an operational environment. Our review focused on Developer Security Testing, which was part of the CADE 2 Security Control Assessment.

The Cybersecurity organization will conduct the Developer Security Testing activity<sup>8</sup> in coordination with other IRS supporting organizations to ensure the CADE 2 TS1 meets the established security requirements in accordance with IRM guidelines and National Institute of Standards and Technology Special Publication 800-53 (NIST SP 800-53), *Recommended Security Controls for Federal Information Systems and Organizations*.<sup>9</sup> This activity is the process of exercising one or more system components under specified conditions to compare actual test results to expected outcomes. Due to the critical nature of the CADE 2 system, the IRS is moving forward with systems security under a short term Authorization to Operate through July 30, 2012; however, the following issues need to be resolved before the CADE 2 system is placed in service.

#### **Management of security requirements testing needs improvement**

IRM 2.6.1 provides guidelines for the development of requirements, tracing those requirements to their sources and test cases, and execution of test cases. It specifies failed test cases should be re-executed in regression testing to ensure no new errors are created by the correction. Additionally, the CADE 2 DI TS1 Developer Security Testing Test Plan provides IRM and NIST SP 800-53 requirements guidance for security testing standards and procedures.

The CADE 2 Application System Security Plan addressed NIST SP 800-53 security controls; however, we identified areas for needed improvements in Developer Security Testing.

- Testing of Developer Security Testing requirements – During sample selection of these requirements, the IRS could not identify and provide complete traceability of test cases to security requirements. The Cybersecurity team performed an analysis tracing test cases to security requirements. As a result, their analysis identified that 219 (72 percent) of 303 security requirements were not tested. The Cybersecurity organization noted in meetings with us that their intent was not to test 100 percent of all security requirements

---

<sup>8</sup> The Cybersecurity organization conducted its Developer Security Testing activity only for the CADE 2 database.

<sup>9</sup> NIST, NIST SP 800-53 Rev. 3, *Information Security: Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009) (includes updates as of May 1, 2010).



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

but to focus on the most critical controls. However, we are concerned with the high percentage of system security requirements not tested at the time of our review.

- Regression testing of failed Developer Security Testing test cases – Based on our review, the CADE 2 Developer Security Testing End of Test Results Report identified that 54 (47 percent) of 115 test cases failed. The 54 failed test cases were categorized into 16 findings based on NIST SP 800-53 control identification numbers. Further analysis by the IRS allowed the 16 findings to be grouped into five risks scheduled for completion in February 2012.

The IRS did not ensure the testers followed the IRM guidelines for development, tracing, and testing of security requirements. The Cybersecurity organization applied NIST SP 800-53 Developer Security Testing guidance and the IRS's annual controls assessment methodology to develop Developer Security Testing test cases, security control traceability, and security testing. In December 2011, the IRS indicated that while not all security requirements would be tested as part of its Developers Security Testing, 100 percent of all applicable NIST SP 800-53 security controls would be tested in the Security Control Assessment before the CADE 2 DI project received its final Authorization to Operate in July 2012. However, CADE 2 officials acknowledged our finding and agreed clarification at the enterprise-wide level is needed to guide processes for systems security requirements testing. We believe that if test case development, security control traceability, and security testing focuses only on required NIST SP 800-53 controls and system components, the risk of missing security requirements could have an adverse impact on CADE 2 functionality and successful implementation. Adequate system security is needed to prevent the loss of Personally Identifiable Information and other sensitive data, maintain taxpayers' trust, and support tax administration functions within the IRS.

### **Vulnerability detection scans identified critical issues in the database management system**

The IRM states that identified vulnerabilities should be corrected within a specific time period, based on criteria in NIST Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*.<sup>10</sup> If the vulnerabilities are not corrected within the specified time period, the IRS needs to add the weaknesses to a Plan of Actions and Milestones so they can be tracked and managed.

The IRS introduced the Guardium solution<sup>11</sup> to perform database vulnerability detection scans. In December 2011, the IRS performed a Guardium scan on the mainframe database management system, which included the four CADE 2 environments: 1) Final Integration Test, 2) Systems

---

<sup>10</sup> NIST, FIPS PUB 199, *FIPS Publication: Standards for Security Categorization of Federal Information and Information Systems* (Feb. 2004).

<sup>11</sup> IBM InfoSphere Guardium's Vulnerability Assessment solution scans database infrastructures on a scheduled basis to detect vulnerabilities and suggests remedial actions.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

Acceptance Test, 3) Development, and 4) Production. Within this database management system are multiple applications and databases, including CADE 2.

The Guardium scan identified a total of 282 issues across the four environments. While the weaknesses specific to the CADE 2 system could not be identified, the issues identified are consistent within each environment. Identified issues are categorized as critical, major, and minor. Of the 282 issues identified, 208 issues are deemed critical. We reviewed only the critical issues identified by the Guardium scan.

- Critical access privilege issues related to users, system accounts, and services with unauthorized access to privilege functionalities account for 202 of the 208 issues.
- Critical issues related to database configuration account for six of the 208 issues. These six configuration issues are related to default databases that were not removed and default ports that were active. The IRM states that default sample databases, along with any associated objects and user accounts, are to be removed. These default databases utilize default user identifications, passwords, and ports, which increase the risk of unauthorized users gaining access to sensitive taxpayer information.

We are concerned that the IRS does not have a fully developed enterprise-wide process in place to address the database weaknesses identified by the Guardium software. While a formal process for reviewing and resolving the scan results known as the Database Vulnerability Remediation Process has been developed, it has not been finalized or approved. The IRS reports that the process is currently being refined on Tier 2 systems before application to Tier 1.

Lastly, the IRS should ensure that a Plan of Actions and Milestones is created within 60 days after the final Authorization to Operate for the CADE 2 DI project to correct any database vulnerability weakness or accept the risk. If this does not occur, the vulnerabilities cannot be tracked and may not be resolved. Again, adequate system security is needed to prevent the loss of Personally Identifiable Information and other sensitive data, maintain taxpayers' trust, and support tax administration functions within the IRS.

### **Source code security review testing identified security weaknesses in the Java Balance and Control Initialization Code**

Encryption standards are mandatory for all Federal Government systems in accordance with FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*.<sup>12</sup> Password policies are set by the IRS in *Application and Operating System Password Policies*, issued November 25, 2011. In addition, correcting computer source coding issues is a best practice applicable to the CADE 2 system.

---

<sup>12</sup> NIST, FIPS PUB 140-2, *FIPS Publication: Security Requirements for Cryptographic Modules* (May 2001). This publication provides a standard to be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

The IRS performed a Source Code Security Review of the JAVA programming code in the CADE 2 Balance and Control Module in October 2011. The IRS stated that this module is used to initialize the CADE 2 database and will be removed once it is initialized. The code review identified 12 issues. Examples of these weaknesses are:

- Encryption standards compliant with FIPS Publication 140-2 are not being used. The application is using a cryptographic algorithm that is not compliant with Federal requirements. The application is using MD5 to generate a hash of the configuration files.
- Data input validation was not being performed, which introduced standard query language injection problems. Standard query language injection occurs when a user is able to enter malicious data that, when included as part of the query, modify the original query to provide additional functionality not intended by the application. This issue is partially mitigated because the source of the data moving through this module is from the IMF database and not from user input.
- Incorrect logical operators were used in conditional statements, leading to potentially invalid results and inappropriate access. One example provided by the Code Review team indicated that when saving a file located on the server, the application attempts to verify that the file exists and the user has the appropriate privileges to write to the file. However, the code as written treats the condition as an “OR” clause, so that only one of the conditions has to be met. Once the program determines that the file exists, it will ignore the rest of the statement and attempt to save the file, which will cause system permission errors if the user does not have write permission on the file.
- Password policy settings required by the IRS were not being used. Although the database credentials are encrypted in the configuration files, the username and password appear to be the same value, which is a violation of IRS password requirements. Additionally, since they are the same value, it would be unlikely that the password being used is sufficient to meet IRS standards because that would mean that the username contained upper case and lower case letters, numbers, and special characters. Further, passwords would need to be changed every 90 days; something that is not true of usernames.

Discussions with the IRS in January 2012 indicated that these issues were not yet addressed and a date to correct the weaknesses had not been scheduled. Throughout this audit we discussed with the IRS the need to better ensure that adequate system security is provided for the CADE 2 system in order to minimize risks with the loss of Personally Identifiable Information and other sensitive data, maintain taxpayers’ trust, and support critical tax administration functions.



---

*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

## **Recommendations**

The Chief Technology Officer should ensure:

**Recommendation 6:** All security requirements and corresponding test cases are identified and sufficiently traced, managed, and tested prior to the CADE 2 DI project implementation to ensure the CADE 2 system operates as intended.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated it has implemented a trace relationship capability in the CADE 2 Program's requirements repository. This capability allows the traceability of security requirements to test case identifiers and provides verification for ensuring that all security requirements for the CADE 2 DI are tested. Moving forward, the IRS plans to input test cases into Rational Quality Manager. Rational Quality Manager will provide an automated means to directly trace test cases to security requirements, thus allowing for proper traceability management for security requirements to test cases.

**Recommendation 7:** All database issues identified by the Guardium scan are resolved or an action plan is developed with specific corrective actions and time periods.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated that the Cybersecurity organization worked with Enterprise Operations using an ad hoc process to triage the initial vulnerability findings, and a formal process is currently under development.

**Recommendation 8:** All issues identified by Source Code Security Review scans are resolved or an action plan is developed with specific corrective actions and time periods prior to the code being placed into service.

**Management's Response:** The IRS agreed with this recommendation. The IRS stated that enterprise-wide, all issues identified by Source Code Security Review scans should be resolved or a remediation action plan be developed prior to putting specific code in service, absent a risk-based decision by the Program Governance Board. The IRS also stated that, in the case of CADE 2 Java Balance and Control Initialization Code, we did not mention in the audit report that an explicit, risk-based decision was made by the CADE 2 Program Governance Board to accept the code weaknesses related to the Program. Since we completed audit fieldwork in January 2012, the IRS has continued to perform secure code reviews within the Program.



---

*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

## **Appendix I**

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

Our overall objective was to determine whether CADE 2 TS1 testing activities were performed in accordance with applicable policies and procedures. To accomplish this objective, we:

- I. Requirements Management – Determined whether the CADE 2 requirements management activities follow systems development guidelines.
  - A. In accordance with audit recommendations in our CADE 2 PMO report,<sup>1</sup> determined the status of requirements and the requirements repository (ReqPro) used to document and control requirements.
  - B. Determined whether a complete RTVM has been developed by the CADE 2 PMO prior to testing, in accordance to IRM 2.6.1.
  - C. For each type of test listed in the audit plan, determined whether the RTVM is updated to reflect test case results.
- II. Testing and Deployment – Determined whether the CADE 2 testing activities met IRM guidelines and industry standards.
  - A. Determined whether the Final Integration Test Phase 1, Systems Acceptance Test, Final Integration Test Phase 2 (2012 Filing Season), and User Acceptance Test were conducted, results analyzed, and defects adequately resolved.
    1. Obtained and reviewed the test plan to ensure it met IRM requirements.
    2. Determined whether defects identified during testing were resolved.
    3. Judgmentally<sup>2</sup> selected and reviewed 49 of 3,083 approved CADE 2 system requirements and 48 of 1,530 unapproved CADE 2 system requirements to determine whether testing activities complied with IRM guidelines and industry standards. We used a judgmental sample because we were not planning to project our results.
    4. Obtained and reviewed the Final Integration Test Phase 1 end-of-test report, which contains the final complete test results.

---

<sup>1</sup> Treasury Inspector General for Tax Administration, Ref. No. 2011-20-127, *Customer Account Data Engine 2 Program Management Office Implemented Systems Development guidelines; However, Process Improvements Are Needed to Address Inconsistencies* (Sept. 2011).

<sup>2</sup> A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

- B. Conducted on-site test observations of the CADE 2 testing to determine whether adequate resources (such as equipment, staff, *etc.*) were assigned, system developers were not performing the testing, testers fully completed the test scripts assigned, and tests results were accurately recorded.
- III. Security – Determined whether the System Security Plan for the CADE 2 system included adequate security controls and whether security testing activities performed prior to deployment met NIST and IRM requirements guidance and industry standards.
- A. Obtained the System Security Plan to determine whether adequate security controls were in place.
  - B. Obtained Developer Security Test testing results to verify that the security controls included in the System Security Plan were successfully tested.
  - C. Obtained Accessibility Test testing results to verify that the security controls included in the System Security Plan were successfully tested.
  - D. For any other security tests identified during the audit, obtained testing results to verify that the security controls adequately met applicable security guidance.
- IV. Configuration Testing – Determined the adequacy of the configuration management of the CADE 2 operating system and associated databases in accordance with NIST, IRM, and other Federal guidance.
- A. Assessed the adequacy of IRS configuration management processes over the CADE 2 operating system and associated databases in both test and production environments.
  - B. Interviewed CADE 2 operating system and database management personnel to determine reasons for variances from the standards, if any.

### **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: IRM and related IRS guidelines and the processes followed in the development of information technology projects. We evaluated these controls by conducting interviews with management and staff, attending meetings of the CADE 2 Test Program and project teams, attending on-site tests, and reviewing Program documentation such as the CADE 2 Program Test Plan, CADE 2 Requirements Management Plan, various test plans, and other documents that provided evidence of whether IRS systems testing processes were followed and whether those processes were adequate.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

## **Appendix II**

### *Major Contributors to This Report*

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)  
Gwendolyn A. McGowan, Director (Systems Modernization and Applications Development)  
Danny R. Verneuille, Director  
Kimberly R. Parmley, Audit Manager  
Larry W. Reimer, Information Technology Audit Manager  
Suzanne M. Westcott, Lead Auditor  
Charlene L. Elliston, Senior Auditor  
Louis Lee, Senior Auditor  
Wallace C. Sims, Senior Auditor  
David F. Allen, Senior Program Analyst  
Hung Q. Dam, Information Technology Specialist  
Arlene Feskanich, Information Technology Specialist  
K. Kevin Liu, Information Technology Specialist



---

*Customer Account Data Engine 2 (CADE 2): System  
Requirements and Testing Processes Need Improvements*

---

**Appendix III**

*Report Distribution List*

Commissioner C  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Deputy Commissioner for Services and Enforcement SE  
Commissioner, Wage and Investment Division SE:W  
Deputy Chief Information Officer for Strategy/Modernization OS:CTO  
Associate Chief Information Officer, Applications Development OS:CTO:AD  
Associate Chief Information Officer, Cybersecurity OS:CTO:C  
Associate Chief Information Officer, Modernization – Program Management Office  
OS:CTO:MP  
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 Liaisons:  
    Commissioner, Wage and Investment Division SE:W:S:PRA:PEI  
    Director, Risk Management Division OS:CTO:SP:RM



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

**Appendix IV**

*Glossary of Terms*

<b>Term</b>	<b>Definition</b>
Applications Development Organization	The IRS organization responsible for building, testing, delivering, and maintaining integrated information applications systems, <i>i.e.</i> , software solutions, to support IRS modernized systems and the production environment.
Authorization to Operate	A formal declaration by a Designated Approving Authority that authorizes operation of a business product and explicitly accepts the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals based on the implementation of an agreed-upon set of information security controls.
Bidirectional Traceability	Bidirectional traceability of requirements can be established from the source requirement to its lower level requirements and from the lower level requirements back to their source. Such bidirectional traceability helps determine that all source requirements have been completely addressed and that all lower level requirements can be traced to a valid source. Also, once test cases are developed for associated requirements, bidirectional traceability enables requirements to trace to test cases and test cases to trace to requirements.
CADE 2 Transition State 1 Solution	Modifies the IMF from a weekly cycle to daily processing, establishes a new relational database to store all individual taxpayer account information, and provides management tools to more effectively use data for compliance and customer service. See Customer Account Data Engine.
Change Request	The medium for requesting approval to change a baselined requirement, product, or other controlled item.
Configuration	The overall way a computer is set up that pertains to hardware and software.
Cryptographic Algorithm	An encrypted or unreadable list of instructions, procedures, or formulas used to solve a problem.
Customer Account Data Engine	A major component of the IRS's Modernization Program. The system consists of current and planned databases and related applications that work with the IRS Master File system (see Master File).
Customer Requirement	Requirements that describe a business or technical need, such as desired functionality, acceptable performance, storage capacity, or system availability and reliability, in the language of the customer.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Term	Definition
Daily Processing Project	A project under the CADE 2 Program that, when completed, will change weekly individual taxpayer account processing to daily processing.
Database	The CADE 2 developed a centralized relational database. A relational database is a collection of data items organized as a set of formally described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables.
Database Implementation Project	A project under the CADE 2 Program intended to implement the newest version of the relational database.
Database Management System	A collection of programs that can store, modify, and extract information from a database.
Developer Security Test (SA-11)	Addresses confidentiality, integrity, and availability of the software; data processed by the system; and resolution of issues that could result in security vulnerabilities.
Encryption	The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to its contents.
Enterprise Architecture	A unifying overall design or structure for an enterprise that includes business and organizational aspects of the enterprise as well as technology aspects. Enterprise Architecture divides the enterprise into its component parts and relationships and provides the principles, constraints, and standards to help align business area development efforts in a common direction. An Enterprise Architecture ensures that subordinate architectures and business system components developed within particular business areas and multiple projects fit together into a consistent, integrated whole.
Enterprise Life Cycle	A structured business systems development method that requires the preparation of specific work products during different phases of the development process.
Federal Information Processing Standards	A set of standards that describe document processing, encryption algorithms, and other information technology standards for use within nonmilitary Government agencies and by Government contractors and vendors who work with the agencies.
Filing Season	The period from January 1 through April 15 when most individual income tax returns are filed.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Term	Definition
Final Integration Test Phase 1	For the CADE 2 system, the Final Integration Test will be conducted in two phases – Phase 1 and Phase 2. Phase 1 has been added to the testing life cycle to accelerate the timing of integrated system testing and provide additional time to take corrective action for any issues that might be identified. Phase 1 will be performed to validate the weekly cycle change, data migration, system integration, systems monitoring and trouble handling, balance and control, operations automation/scheduling, and system performance.
Final Integration Test Phase 2	For the CADE 2 system, the Final Integration Test will be conducted in two phases – Phase 1 and Phase 2. Phase 2 will be a “traditional” filing season Final Integration Test that includes the 2012 Filing Season and legislative changes. The Final Integration Test is the integrated end-to-end testing of multiple systems that support the high-level business requirements of the IRS. It is designed to ensure that IRS systems interoperate correctly prior to production startup utilizing copies of production data in a near-production environment. The Final Integration Test is performed from the perspective that all IRS application systems are subsystems to an overall Tax Processing System. The Tax Processing System consists of hundreds of subsystems operating on many unique hardware and software platforms. The Final Integration Test verifies that data are transferred correctly between the systems within the Tax Processing System.
Hashing	When referring to security, hashing is a method of taking data, encrypting it, and creating unpredictable, irreversible output. There are many different hashing algorithms. MD2, MD5, SHA, and SHA-1 are examples of hashing algorithms.
Individual Master File	The IRS database that maintains transactions or records of individual tax accounts.
Infrastructure	The fundamental structure of a system or organization. The basic fundamental architecture of any system (electronic, mechanical, social, political) determines how it functions and how flexible it is to meet future requirements.
Initiation Phase	The first of four phases of the IRS testing life cycle. The Initiation Phase begins the test planning process to determine the test scope, cost, and schedule. It also includes requirements analysis and the development of the RTVM.
Integrated Data Retrieval System	The IRS computer system capable of retrieving or updating stored information; it works in conjunction with a taxpayer’s account records.
Java Programming Code	Computer program instructions used by computer programmers to develop applications, scripts, or other sets of instructions for a computer to execute.
Logical Operators	Another way of defining the Boolean operators: AND, OR, and NOT. The Boolean operators were developed by the English mathematician and computer pioneer, George Boole.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Term	Definition
Master File	The IRS database that stores various types of taxpayer account information. This database includes individual, business, and employee plans and exempt organizations data.
Milestone	Scheduled time period for providing a “go/no-go” decision point in a program or project (can be associated with funding approval to proceed).
National Institute of Standards and Technology	A nonregulatory Federal agency, within the Department of Commerce, responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.
Personally Identifiable Information	Information that can be used to uniquely identify, contact, or locate a single individual or that can be used with other sources to uniquely identify a single individual.
Plan of Actions and Milestones	A management process that outlines weaknesses and delineates the tasks necessary to mitigate them.
Rational Quality Manager	An application used to manage testing activities, including test cases, across the testing life cycle. Rational Quality Manager was a pilot project for the CADE 2 Program and was not used by all testing partners.
Rational Requisite Pro	An application used for requirements management. The IRS has established ReqPro as its Enterprise Architecture standard for requirements management. It is used to capture detailed requirement data such as the requirement text and any supporting attributes to organize or clarify the requirement. The application also has the capability to create and maintain full requirements traceability within a single project or across multiple projects.
Requirement	A formalization of a need and statement of a capability or condition that a system must have or meet to satisfy a contract, standard, or specification.
Requirements Measures and Metrics Report	Routinely reports on requirements measures and metrics to provide leadership with objective information to evaluate the status of requirements and identify areas for remediation. For example, the requirements measures include requirements volatility, requirements traceability, requirements completeness, <i>etc.</i> The requirements metrics include the total number of requirements, the number of requirements by type, the number of revisions made to requirements, the number of requirements not traced, <i>etc.</i>
Requirements Traceability Verification Matrix	A tool that documents requirements and establishes the traceability relationships between the requirements to be tested and their associated test cases and test results.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Term	Definition
Security Certification and Accreditation	A security certification is an independent technical evaluation, for the purpose of accreditation, that uses security requirements as the criteria for the evaluation. An accreditation is an authorization granted by a management official to operate the system based on the evaluation of the security controls.
Source Code Security Review	The Cybersecurity organization conducts activities designed to ensure a system's security safeguards are in place and functioning as intended. Source code analysis will be used to test CADE 2 application code for potential security vulnerabilities. Source Code Security Review is the process of auditing the source code for an application to verify the proper security controls are present, that they work as intended, and that they have been invoked in all the right places.
Stakeholders	An individual or organization that is materially affected by the outcome of the system. Key stakeholders represent both business and technical functions that fully participate in the architecture development effort to ensure that directional guidance is both accurate and sufficient. These stakeholders are empowered to make project and architectural decisions. Examples of project stakeholders include the customer, the user group, the project manager, the development team, and the testers.
Standard Query Language	A standardized query language for requesting information from a database.
Standard Query Language Injection	A form of attack on a database-driven website in which the attacker executes unauthorized Standardized Query Language commands by taking advantage of insecure code on a system connected to the Internet, bypassing the firewall.
Systems Acceptance Test	A software test to ensure the designed and delivered software has met all system requirements. This is accomplished by validating that the project or system performs as expected when subjected to controlled test cases and data for both valid and invalid conditions.
Test Case	A test case is created to specify and document the conditions to be tested and to validate that system functions meet requirements as translated into documented functional design. A test case also tests outside the normal or expected functions in order to find defects.
Testing Partners	The CADE 2 testing partners are those IRS organizations (Enterprise Systems Testing, Cybersecurity, Applications Development, <i>etc.</i> ) that participate in CADE 2 testing.
Tier 1 system	A system comprised of supercomputers and mainframe hardware and software.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

Term	Definition
Tier 2 system	A system comprised of minicomputers and software, <i>i.e.</i> , computers usually containing multiple microprocessors, capable of executing multiple processes simultaneously and oftentimes serve multiple users by way of a communications network. Local Area Network servers are often located in a space separate from the normal office environment. The minicomputer is more robust than a microcomputer.
Traceability	Describes the life of a requirement from the initial source through its development and actual deployment into operations.
Unified Work Request	Details the requested design and functionality of a system.
User Acceptance Test	A test conducted to validate that the system works as designed and implemented and satisfies the business requirements of the system.
Validation	Verification that something is correct or conforms to a certain standard.
Vulnerability	In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance.
Vulnerability Detection Scans	The Cybersecurity organization conducts activities designed to ensure a system's security safeguards are in place and functioning as intended. Vulnerability Detection Scans verify whether security and privacy mechanisms designed to protect vulnerable areas of the system are configured properly and enforced.



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

**Appendix V**

*Management's Response to the Draft Report*

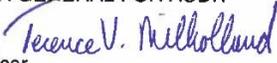


CHIEF TECHNOLOGY OFFICER

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

SEP 11 2012

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland   
Chief Technology Officer

SUBJECT: Draft Audit Report – *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements* (Audit #201120005)  
(e-trak #2012-34684)

Thank you for the opportunity to review your draft audit report and discuss earlier draft observations with the audit team.

I was pleased to read your comments and observations acknowledging the extensive testing performed prior to deployment of CADE 2 Transition State 1. This testing, including the implementation of Final Integration Testing Phase 1, prior to the beginning of the 2012 filing season, significantly decreased the risk of implementing the Daily Processing of tax returns in January 2012. In addition, I appreciate TIGTA acknowledging our use of independent assessments and processing simulation exercises to identify and correct potential issues. This effort helped to ensure the IRS' readiness for the January 2012 Daily Processing deployment.

Overall, I agree with the recommendations provided in this report; however, there are a few instances where the IRS disagrees with TIGTA. In particular, the IRS does not agree with the need for an enterprise-wide policy for RTVM at the program level. The IRS does not believe automated tools are always necessary to maintain control over requirements and test case management, e.g., web services applications, or if provided by other processes.

In addition, the IRS believes that appropriate documentation already exists for infrastructure requirements with the association of Government Equipment Lists and environmental checklists, which provide sufficient assurance that infrastructure components have been acquired and implemented. Thus, we disagree with your recommendation in this area also.

Lastly, we believe that TIGTA should take into account and recognize in their audit report those instances where IRS Governance authorities have made risk-based



*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

2

decisions, such as the acceptance of code weaknesses, based on our assessment of the likelihood of a risk's occurrence.

We are committed to continuously improving our information technology systems and processes. We value your continued support and the assistance and guidance your team provides. If you have any questions, please contact me at (202) 622-6800, or a member of your staff may contact Karen Mayr at (240) 613-1431.

Attachment



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

Draft Audit Report – Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements (Audit #201120005) (e-trak #2012-34684)

**RECOMMENDATION #1:** The Chief Technology Officer should ensure:

- a. Requirements and corresponding test cases are identified and sufficiently traced, managed and tested prior to the CADE 2 Database Implementation to ensure the CADE 2 system operates as intended.
- b. Enhanced oversight of traceability controls are implemented enterprise-wide. This includes developing and providing a program level Requirements Traceability Verification Matrix (RTVM) prior to the test Initiation Phase of Internal Revenue Manual (IRM) 2.6.1, and that the program level RTVM is updated to include test cases and final tests results. This process should be formally documented.
- c. The CADE 2 PMO provides enhanced oversight of traceability controls. This includes developing and providing a program level RTVM prior to the test Initiation Phase of IRM 2.6.1, and that the program level RTVM is updated to include test cases and final tests results. This process should be formally documented.

**CORRECTIVE ACTION #1a:** The IRS agrees with the recommendation. We will ensure requirements and corresponding test cases are identified and sufficiently traced, managed, and tested prior to the CADE 2 Database Implementation.

**IMPLEMENTATION DATE:** June 1, 2013

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion

**CORRECTIVE ACTION #1b & c:** The IRS disagrees with these recommendations. IRS has not committed to enterprise-wide program level RTVM nor program level testing IRMs for using program RTVMs. While IRS agrees with the principle of program-level traceability, we do not agree that it needs to be implemented through an RTVM artifact. IRS has already complied with Recommendation 1c with the development of a CADE 2 Program RTVM. It should be noted that we also disagree with the two recommendations based on inaccuracies in the content of the recommendations, previously pointed out to TIGTA, in that RTVMs are actually prepared during the Test Initiation Phase, not before the Test Initiation Phase.

**IMPLEMENTATION DATE:** Not Applicable

**RESPONSIBLE OFFICIAL:** Not Applicable

**CORRECTIVE ACTION MONITORING PLAN:** Not Applicable.



---

*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

Draft Audit Report – Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements (Audit #201120005) (e-trak #2012-34684)

**RECOMMENDATION #2:** The Chief Technology Officer should ensure:

- a. A standard suite of integrated, automated tools is implemented enterprise-wide to enable programs and projects to develop and manage requirements, develop and manage test cases, bi-directionally trace requirements and test cases, monitor and manage test case defects, and bi-directionally trace test case defects with test cases and requirements.
- b. A standard suite of integrated, automated tools is implemented for CADE 2 Transition State 2 and all future CADE 2 projects to develop and manage requirements, develop and manage test cases, bi-directionally trace requirements and test cases, monitor and manage test case defects, and bi-directionally trace test case defects with test cases and requirements.

**CORRECTIVE ACTION #2a & b:** The IRS disagrees with these recommendations. IRS has not committed to a policy, nor funded a project, to standardize and implement tools on an enterprise-wide level. Neither recommendation offers any flexibility for projects that are not good candidates for automated tools. In addition, automated tools are not always necessary to maintain control over requirements and test cases management, traceability, etc., so we do not agree with TIGTA prescribing their use.

**IMPLEMENTATION DATE:** Not Applicable

**RESPONSIBLE OFFICIAL:** Not Applicable

**CORRECTIVE ACTION MONITORING PLAN:** Not Applicable

**RECOMMENDATION #3:** The Chief Technology Officer should ensure:

IRM guidelines are followed, specifically that:

- a. Test cases and other appropriate documentation are properly developed for infrastructure requirements, and all infrastructure documentation includes complete traceability to the requirements being tested and the testing results.
- b. IRS testers obtain and maintain documentation to verify test results.
- c. Test execution practices are consistent prior to CADE 2 Database Implementation.

**CORRECTIVE ACTION #3a:** The IRS disagrees with this recommendation. We believe that appropriate documentation already exists for infrastructure requirements with the association of Government Equipment Lists and environmental checklists that provide sufficient assurance that infrastructure components have been acquired and implemented.

**IMPLEMENTATION DATE:** Not Applicable

**RESPONSIBLE OFFICIAL:** Not Applicable

**CORRECTIVE ACTION MONITORING PLAN:** Not Applicable



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

Draft Audit Report – Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements (Audit #201120005) (e-trak #2012-34684)

**CORRECTIVE ACTION #3b:** The IRS agrees with this recommendation. We will ensure IRM guidelines are followed, and that IRS testers both obtain and maintain documentation to verify test results.

**IMPLEMENTATION DATE:** March 31, 2013

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.

**CORRECTIVE ACTION #3c:** The IRS agrees with this recommendation. We will ensure IRM guidelines are followed, and test execution practices are consistent prior to CADE 2 Database Implementation.

**IMPLEMENTATION DATE:** March 31, 2013

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.

**RECOMMENDATION #4:** The Chief Technology Officer should ensure the quality review processes, to include customer technical reviews, identify, correct, or remove requirements that could not be tested prior to the implementation of testing activities.

**CORRECTIVE ACTION #4:** The IRS agrees with this recommendation. We will develop procedures to ensure that quality review processes identify, correct, or remove requirements that could not be tested prior to the implementation of testing activities. This will include customer technical reviews.

**IMPLEMENTATION DATE:** March 31, 2013

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.



---

*Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

Draft Audit Report – Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements (Audit #201120005) (e-trak #2012-34684)

**RECOMMENDATION #5:** The Chief Technology Officer should ensure formal change management processes are implemented for all deferred and proposed requirements prior to the CADE 2 Database Implementation.

**CORRECTIVE ACTION #5:** The IRS agrees with this recommendation. We will develop procedures to ensure a formal change management process for all deferred and proposed requirements.

**IMPLEMENTATION DATE:** March 31, 2013

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Enterprise Services

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.

**RECOMMENDATION #6:** The Chief Technology Officer should ensure all security requirements and corresponding test cases are identified and sufficiently traced, managed, and tested prior to the CADE 2 Database Implementation to ensure the CADE 2 system operates as intended.

**CORRECTIVE ACTION #6:** The IRS agrees with this recommendation. We have implemented a trace relationship capability in the program's requirements repository. This capability allows the traceability of security requirements to test case identifiers and provides verification for ensuring that all security requirements for the CADE 2 Database Implementation are tested. Moving forward, we plan to input test cases into Rational Quality Manager (RQM). RQM will provide an automated means to directly trace test cases to security requirements, thus allowing for the proper traceability management for security requirements to test cases.

**IMPLEMENTATION DATE:** Implemented Trace Relationship Capability on November 25, 2011

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Applications Development

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.

**RECOMMENDATION #7:** The Chief Technology Officer should ensure all database issues identified by the Guardium scan are resolved or an action plan is developed with specific corrective actions and timeframes.

**CORRECTIVE ACTION #7:** The IRS agrees with this recommendation. Cybersecurity worked with Enterprise Operations using an ad hoc process to triage the initial vulnerability findings. A formal process is currently under development.



---

## *Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements*

---

Draft Audit Report – Customer Account Data Engine 2 (CADE 2): System Requirements and Testing Processes Need Improvements (*Audit #201120005*) (*e-trak #2012-34684*)

**IMPLEMENTATION DATE:** January 31, 2013

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cyber security

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.

**RECOMMENDATION #8:** The Chief Technology Officer should ensure all issues identified by source code security review scans are resolved or an action plan is developed with specific corrective actions and timeframes prior to the code being placed into service.

**CORRECTIVE ACTION #8:** The IRS agrees with this recommendation. Enterprise-wide, all issues identified by source code security review scans should be resolved or a remediation action plan developed prior to putting specific code in service, absent a risk-based decision by the program Governance Board. In the case of CADE 2 Java Balance and Control Initialization code, TIGTA did not mention in the audit report that an explicit, risk-based decision was made by the CADE 2 Governance Board to accept the code weaknesses related to the program. Since TIGTA completed its fieldwork in January 2012, the IRS has continued to perform secure code reviews within the program.

**IMPLEMENTATION DATE:** December 31, 2012

**RESPONSIBLE OFFICIAL:** Associate Chief Information Officer, Cyber security

**CORRECTIVE ACTION MONITORING PLAN:** We enter accepted Corrective Actions into JAMES. These Corrective Actions are monitored on a monthly basis until completion.