



*Affordable Care Act
Coverage Data Repository: Risks With
Systems Development and Deployment*

June 2, 2015

Reference Number: 2015-23-041

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

Redaction Legend:

2 = Risk Circumvention of Agency Regulation or Statute

Phone Number / 202-622-6500

E-mail Address / TIGTACommunications@tigta.treas.gov

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



HIGHLIGHTS

AFFORDABLE CARE ACT COVERAGE DATA REPOSITORY: RISKS WITH SYSTEMS DEVELOPMENT AND DEPLOYMENT

Highlights

Final Report issued on June 2, 2015

Highlights of Reference Number: 2015-23-041
to the Internal Revenue Service Chief
Technology Officer.

IMPACT ON TAXPAYERS

In March 2010, the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act were enacted. These laws are collectively referred to as the Affordable Care Act (ACA). The ACA is intended to make health insurance more affordable and available to individuals. The IRS is developing the Coverage Data Repository (CDR) to help implement the ACA, and it will be the IRS's sole authoritative source of all ACA data for health care-related functions and services. During the 2015 Filing Season, the IRS will receive Exchange Periodic Data (EPD) from the Exchanges, store the EPD in the CDR, and use the EPD to verify the accuracy of the Premium Tax Credits claimed by taxpayers.

WHY TIGTA DID THE AUDIT

The overall objective was to determine how systems development risks for the CDR Project were being mitigated and whether established business and information technology requirements were being met. Specifically, TIGTA evaluated CDR testing processes, including interagency, release-level, and project-level functional testing controls as well as security and audit trail controls.

WHAT TIGTA FOUND

TIGTA found that risks could not be effectively mitigated by CDR testing processes. Interagency testing with the Federal and State Exchanges was not completed. As of November 21, 2014, the IRS had only received EPD from three States. Subsequent to our

fieldwork, the IRS received additional data, but it still had not yet received all required EPD submissions from the Exchanges as of January 20, 2015, the start of the 2015 Filing Season.

Release-level testing was completed but not prior to initiating interagency testing with the Centers for Medicare and Medicaid Services. During project-level testing, system developers did not always demonstrate CDR functionality to business owners and did not maintain complete records verifying business participation. The CDR was deployed before responsible officials completely assessed security risks and authorized the system to operate. The CDR Application Audit Plan was not implemented as needed to support the IRS's program and policy to mitigate risks for unauthorized access to taxpayers' records.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer: 1) ensure that interagency testing with the Exchanges is completed, 2) ensure that future ACA projects complete release-level testing before starting interagency testing, 3) verify that CDR 2.0 functionality has been adequately demonstrated to ACA business owners, 4) ensure that sufficient evidence is maintained to verify adequate business owner participation, 5) ensure that authorizing officials evaluate and accept CDR risks prior to deployment, and 6) ensure that the CDR Application Audit Plan is completed, approved, sufficiently tested, and implemented.

In management's response to the report, the IRS agreed with two of TIGTA's recommendations. However, the IRS disagreed with three of TIGTA's recommendations and partially disagreed with a fourth. The Chief Technology Officer did not concur with recommendations to strengthen systems testing practices nor with TIGTA's assessment of the process applied to demonstrate and verify system functionality for the CDR. Because the IRS plans to rely on the CDR as its sole authoritative source for all ACA data, TIGTA maintains that improvements are needed to ensure adequate risk mitigation practices in each of these areas.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

June 2, 2015

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment
(Audit #201420310)

This report presents the results of our review of how the Internal Revenue Service (IRS) managed systems development controls over the Affordable Care Act¹ Coverage Data Repository Project (CDR). The overall objective of this review was to determine whether the IRS is adequately mitigating systems development risks under the Affordable Care Act Program to achieve business and information technology goals for the CDR Release 2.0 Project. Specifically, we evaluated the IRS's key risk management controls and processes for project management, testing, and security for the CDR Release 2.0 Project. This audit was included in the Treasury Inspector General for Tax Administration's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Implementing the Affordable Care Act and Other Tax Law Changes.

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

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

¹ Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029. See Appendix VII for a glossary of terms.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Table of Contents

Background	Page 1
-------------------------	--------

Results of Review	Page 9
--------------------------------	--------

Risks Could Not Be Effectively Mitigated by Testing Processes Planned for the Coverage Data Repository	Page 9
---	--------

<u>Recommendation 1</u> :	Page 12
---------------------------------	---------

<u>Recommendation 2</u> :	Page 14
---------------------------------	---------

<u>Recommendation 3</u> :	Page 16
---------------------------------	---------

<u>Recommendation 4</u> :	Page 17
---------------------------------	---------

Improved Controls Are Needed to Ensure That Only Approved Applications Are Deployed Into the Internal Revenue Service's Production Environment	Page 18
--	---------

<u>Recommendation 5</u> :	Page 19
---------------------------------	---------

The Coverage Data Repository Audit Plan Was Not Implemented to Support the Internal Revenue Service's Unauthorized Access to Taxpayers' Records Program	Page 19
---	---------

<u>Recommendation 6</u> :	Page 23
---------------------------------	---------

Appendices

Appendix I – Detailed Objective, Scope, and Methodology	Page 24
---	---------

Appendix II – Major Contributors to This Report	Page 26
---	---------

Appendix III – Report Distribution List	Page 27
---	---------

Appendix IV – Exchange Periodic Data Elements	Page 28
---	---------

Appendix V – Coverage Data Repository 2.0 Systems Development and Testing Timeline	Page 30
---	---------

Appendix VI – Coverage Data Repository High-Level Logical System Architecture	Page 32
--	---------

Appendix VII – Glossary of Terms	Page 33
--	---------

Appendix VIII – Management's Response to the Draft Report	Page 36
---	---------



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Abbreviations

ACA	Affordable Care Act
CDR	Coverage Data Repository
CMS	Centers for Medicare and Medicaid Services
EPD	Exchange Periodic Data
HHS	Department of Health and Human Services
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
IT	Information Technology
SSN	Social Security Number
TIGTA	Treasury Inspector General for Tax Administration
UNAX	Unauthorized Access



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

Background

In March 2010, the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act¹ were enacted. These laws are collectively referred to as the Affordable Care Act (ACA). The ACA is intended to make health insurance more affordable and available to individuals. The ACA seeks to:

- Provide more Americans with access to affordable health care by creating new Health Insurance Exchanges (commonly referred to as Marketplaces);
- Enforce patient/consumer protections; and
- Provide Government subsidies for people who cannot afford insurance.

The Exchanges are intended to provide a place for Americans to shop for health insurance in a competitive environment. The term Exchanges refers to the Federal Exchange, the State Partnership Exchanges, and the State Exchanges. To enroll in health insurance coverage offered through an Exchange, individuals must complete an application and meet certain eligibility requirements defined by the ACA. Individuals began using the Exchanges on October 1, 2013, to purchase health insurance for Calendar Year 2014. As of December 8, 2014, 20 States use the Federal Exchange, 14 States operate as State Partnership Exchanges, and 16 States and the District of Columbia operate as State Exchanges.

The Department of Health and Human Services/Centers for Medicare and Medicaid Services (HHS/CMS)² oversees implementation of certain ACA provisions related to the Exchanges. The CMS operates the Federal Exchange and works with States to establish State Exchanges and State Partnership Exchanges, including overseeing their operations. The Exchanges have sole responsibility for determining if an individual is eligible to purchase health insurance through the Exchange.

The Internal Revenue Service (IRS) administers the law's numerous tax provisions. The IRS estimates that the ACA includes approximately 50 tax provisions and at least eight of the 50 provisions require the IRS to build new computer applications and business processes that do not exist within the current tax administration system.

¹ Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.

See Appendix VII for a glossary of terms.

² The CMS is a division of the HHS.



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

The IRS established the Information Technology (IT) ACA Program Management Office to ensure a dedicated focus on fulfilling the ACA requirements. Specifically, the IT ACA Program Management Office is responsible for planning and managing information technology responsibilities related to ACA implementation and the myriad of legislative requirements. The IT ACA Program Management Office has developed a multiyear ACA information technology release strategy to support information technology systems development. Some of these releases are operational and in production, while others are in various stages of development and are scheduled for deployment over the next several years. This systems development strategy includes new information technology development as well as modifications to current IRS systems. Figure 1 summarizes the IRS's ACA releases and descriptions.

Figure 1: Summary of the IRS's ACA Releases and Their Respective Descriptions

ACA Release	Deployment Date	Description
ACA 1.0	January 2010 - January 2011	Included the functionality of several ACA provisions, e.g., the Small Business Health Care Tax Credit and the Charitable Hospital Reporting provisions.
ACA 2.0/2.4	July 2011 - June 2013	Included functionality to support the Branded Prescription Drug provision of the ACA and updates to previously released ACA projects.
ACA 3.0	October 2013	Supports the eligibility and enrollment of the Exchange programs by providing income and family size information from the most recently filed tax return and by providing a calculation of Maximum Advance Premium Tax Credit upon request from the HHS Data Services Hub.
ACA 4.0	September 2014	Receives and stores the Exchange Periodic Data (EPD) from the Exchanges and prepares for filing and post-filing compliance activities.
ACA 4.1	March – October 2014	Calculates and collects annual fees based on reports provided by health insurance providers and pharmaceutical manufacturers.
ACA 5.0	November 2014 – January 2015	Will validate ACA forms and perform at-filing compliance activities.
ACA 6.0/6.1	January 2015 - Late 2015	Includes the functionality of post-filing compliance.
ACA 7.0 – 9.0	January 2016 - June 2018	Focuses on supporting IRS compliance activities for the 2016 and 2017 Filing Seasons.

Source: ACA Implementation, ACA Orientation for Treasury Inspector General for Tax Administration (TIGTA) (Marketplace Focus) dated March 12, 2014; TIGTA, Ref. No. 2014-23-072, Affordable Care Act: Improvements Are Needed to Strengthen Security and Testing Controls for the Affordable Care Act Information Returns Project (Sept. 2014); IRS Fiscal Year 2015 Budget Request; and the IT ACA Program Management Office Program Governance Board Briefing dated December 8, 2014.



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

The Coverage Data Repository (CDR) is one of six core systems identified by the IRS that it is developing to implement the ACA legislation. The Draft CDR Business Systems Report dated August 29, 2013, jointly developed by the IT ACA Program Management Office and the Office of Services and Enforcement's ACA Program Office (hereafter referred to as simply the ACA Program Office), states that the CDR database is the IRS's sole authoritative source of all ACA data for health care-related functions and services. The draft report explains that external ACA data from the CMS and the Exchanges will be stored in the CDR. The CDR will be used by all IRS ACA systems to store and retrieve data.

The draft report also states that IRS nonexchange ACA systems, such as the Branded Prescription Drugs and Insurance Provider Fees systems, will not interface and interact with the CDR. The IRS estimates that ACA implementation will cost nearly \$2 billion over the development life cycle. By the end of Fiscal Year 2014, the IRS had spent nearly \$85.8 million of the estimated \$2 billion to fund implementation of the CDR.

ACA 4.0 incorporates CDR Release 2.0 and spans three ACA business areas, including eligibility and enrollment, exchange information processing, and data analytics and reporting. Figure 2 summarizes the business areas, functions, and capabilities planned for ACA 4.0.

Figure 2: Summary of the ACA 4.0 Business Areas, Functions, and Capabilities

ACA Business Area	Business Function	Business Capability
Eligibility and Enrollment	Income and Family Size Verification	<ul style="list-style-type: none">Ability to electronically receive the request for the Income and Family Size Verification from the HHS.
	Maximum Advance Premium Tax Credit Determination	<ul style="list-style-type: none">Ability to receive data from the HHS to estimate the Maximum Advance Premium Tax Credit.Ability to send the estimated Maximum Advance Premium Tax Credit to the HHS.
Exchange Information Processing	EPD Submission	<p>EPD Submission</p> <ul style="list-style-type: none">Ability to receive and intake the EPD via the HHS Data Services Hub.Ability to apply data quality and consistency checks to the EPD.Ability to complete system-level checks and validate that the data are in the appropriate format and complete.Ability to store the EPD.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

ACA Business Area	Business Function	Business Capability
Data Analytics and Reporting	Management Reporting	<p>Performance Management, Analysis, and Reporting</p> <ul style="list-style-type: none">• Ability to select the relevant data necessary for reporting and analysis, including ACA-related information.• Ability to conduct reporting and analysis using the EPD.• Education and outreach reporting.

Source: ACA Program Baseline Requirements, Solution Architecture, and the IT Roadmap dated August 29, 2014.

The following describes each of the four business functions.

1. Income and Family Size Verification Information. For 2015 open enrollment beginning in October of 2014, the IRS supports synchronous (near real-time transactions) and asynchronous (bulk) Income and Family Size Verification³ transactions. ACA 4.0 focuses on the expansion of Income and Family Size Verification transactions and implementation of bulk processing services to include all individuals receiving an eligibility determination and purchasing exchange coverage. The Exchanges submit requests to the IRS using the HHS Data Services Hub to obtain an applicant's Income and Family Size Verification information. The Exchange provides the Social Security Number (SSN), full name, and relationship to the tax filer for all individuals on the application. In response, the IRS provides tax return information for applicants and their family members to the Exchanges via the HHS Data Services Hub. The Exchange uses the information provided to assist in predicting an applicant's income and family size for the requested health coverage period and determine eligibility to receive the Advance Premium Tax Credit. The Exchange is not required to use the information the IRS provides.

2. The Advance Premium Tax Credit. ACA 4.0 adds asynchronous bulk processing for the population that enrolls in Exchange health plans. Eligible individuals who purchase health insurance through the Exchanges may be eligible for and request a refundable tax credit (the Premium Tax Credit) to assist with paying their health insurance premiums. Individuals may elect to have an Advance Premium Tax Credit paid directly to their health insurance provider as partial payment for their monthly premiums or receive the Premium Tax Credit as a lump-sum credit on their annual Federal tax return at the end of each coverage year beginning with Tax Year 2014. Starting in January 2015, individuals must include the amount of any Advance Premium Tax Credit on their tax return and reconcile it to the allowable amount of Premium Tax

³ For more details about Income and Family Size Verification, see TIGTA report Ref. No. 2014-43-044, *Affordable Care Act: Accuracy of Responses to Exchange Requests for Income and Family Size Verification Information and Maximum Advance Premium Tax Credit Calculation* (Jul. 2014).



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

Credit. Each month, the Exchange uses the HHS Data Services Hub to transmit the amount of Advance Premium Tax Credit as part of its EPD. According to the IRS, the Electronic Fraud Detection System is the fraud detection system of record for the ACA in the 2015 Filing Season.

3. EPD Submission. The EPD is taxpayer health care information provided by the Exchanges. ACA 4.0 functionality allows the IRS to begin receiving month-by-month EPD reports from the Exchanges through the HHS Data Services Hub. During the 2015 Filing Season, the IRS will use the EPD in at-filing and post-filing compliance activities.

4. Management Reporting. ACA 4.0 provides the ability to conduct more integrated and complex analysis and reporting on the EPD. The ACA reporting strategy is built primarily for ad hoc and periodic reporting purposes. Reporting will assist customer service outreach activities and statistical analysis.

The CDR systems development project includes a series of four releases with full implementation currently scheduled for June 2015. Figure 3 summarizes planned CDR functionality by ACA and CDR release.

Figure 3: Summary of the CDR Functionality by ACA and CDR Release

ACA/CDR Release	Deployment Date	Functionality
ACA 3.0 CDR 1.0	October 2013	<ul style="list-style-type: none">Provides a centralized ACA data repository.Collects and consolidates ACA data.The IRS uses the data contained in the CDR to respond to Income and Family Size Verification information requests from the Exchanges.
ACA 4.0 CDR 2.0	September 2014	<ul style="list-style-type: none">Supports the increased EPD flows from the HHS Data Services Hub into the IRS's CDR.Allows the IRS to prepare for filing and post-filing compliance activities.
ACA 5.0 CDR 3.0	January 2015	<ul style="list-style-type: none">Enables at-filing checks of tax returns reporting a Premium Tax Credit.
ACA 6.1 CDR 4.0	Mid-Late 2015	<ul style="list-style-type: none">Provides additional Income and Family Size Verification data and the Advance Premium Tax Credit Failure to Reconcile Flag to support health care exchange eligibility.

Source: ACA Program Release Schedule dated February 26, 2012; IRS Fiscal Year 2015 Budget Request; Draft CDR Business System Reports dated June 27, 2014, and August 29, 2013; TIGTA, Ref. No. 2014-43-044, Affordable Care Act: Accuracy of Responses to Exchange Requests for Income and Family Size Verification Information and Maximum Advance Premium Tax Credit Calculation (July 2014); and IRS IT ACA Program Management Office Briefing to the Chief Technology Officer dated October 3, 2014.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

CDR Release 1.0 – In September 2013, the IRS loaded taxpayer data from the Individual Master File, the Individual Return Transaction File, and the Data Master One file. The CDR will store a maximum of two years of a taxpayer’s data at any time. The CDR will contain current tax year and previous tax year information for all taxpayers. The IRS uses the data contained in the CDR to respond to Income and Family Size Verification information requests from the Exchanges.

CDR Release 2.0 – In September 2014, the IRS deployed ACA 4.0/CDR 2.0, which implemented functionality to enable the IRS to receive the EPD from the Exchanges on a monthly basis. The IRS began receiving the EPD from the Exchanges in October 2014. Each month of the EPD is cumulative, containing data from all the prior months of that coverage year. The Exchanges submit the EPD through the HHS Data Services Hub to the IRS. After successful validation, the EPD, both clean data and data with errors, are passed to the CDR database. Prior to loading the EPD into the CDR, a series of data consistency checks are conducted outside of the CDR that were not included in the scope of our review. *****2*****
*****2*****
*****2*****. Appendix VI depicts the CDR high-level logical system architecture and reflects functional components that are part of or interact with the CDR.

According to the Draft CDR Business System Report dated June 27, 2014, the business owner and primary stakeholder for the CDR is the ACA Program Office. The mission of the ACA Program Office is to support the administration of the tax provisions of the ACA through collaboration with government agencies and other stakeholders. ACA administration encompasses the planning, development, and implementation of information technology systems needed to support the IRS’s tax administration responsibilities associated with key provisions of the ACA legislation. The ACA Program Office relies on the Advance Premium Tax Credit payment data received, as part of the monthly EPD, to validate Premium Tax Credit claims.

The CDR Project is following the IRS’s Enterprise Life Cycle Iterative Path for systems development. The Iterative Path is considered an agile⁴ approach to systems development and is suited for projects that change quickly and have requirements that are undefined. The Iterative Path facilitates development of the defined requirements while other requirements are being established. Under the Iterative Path, a process known as “sprints” develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. Appendix V details a timeline for CDR 2.0 systems development and testing. Figure 4 describes the CDR 2.0 processes and how the EPD will be used to support ACA tax provisions.

⁴ The IRS applies the term “agile” to represent a type of software development methodology based on iterative and incremental methods that promote teamwork, collaboration, and process adaptability throughout the life cycle of the project.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Figure 4: CDR 2.0 Business Processes and How the Data Are Used

CDR 2.0 Business Process	Data Used	How Data Are Used
Store Transactional Data	Household income and family size based on taxpayer records	The IRS uses the data to calculate the household income, and the Exchanges will use the household income and family size information based on taxpayer records to make an assistance determination.
Retrieve Individual Record	Household income and family size	The IRS provides the household income/family size of the primary applicant and sends this information to the Exchanges via the HHS Data Services Hub. This information will be gathered using tax records and determining filing status, family size, dependents, and modified adjusted gross income of the primary applicant. The Exchanges will use the household income and family size information based on taxpayer records to make an assistance determination.
Store Transactional Data	Income and Family Size Verification Redetermination Data	Data are stored in the CDR for later use by Income and Family Size Verification redetermination processes.
Store Transactional Data	<p>The EPD will contain the following data:</p> <ul style="list-style-type: none"> • Individual • Employer Entity • Household Coverage • Individual Policy • Exemption • Advance Premium Tax Credit Payment • Small Business Health Options Employer • Small Business Health Options Employee 	The IRS will use data in at-filing and post-filing compliance activities.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

CDR 2.0 Business Process	Data Used	How Data Are Used
Perform Extract, Transform, and Load Activities (Incoming)	Household income and family size information based on taxpayer records	The IRS will use the data to calculate the household income, and the Exchanges will use household income and family size information based on taxpayer records to make an assistance determination.
Perform Extract, Transform, and Load Activities (Outgoing)	Household income and family size	The IRS provides the household income and family size of the primary applicant and sends this information to the Exchanges via the HHS Data Services Hub. This information shall be gathered using tax records and determining filing status, family size, dependents, and modified adjusted gross income of the primary applicant. The Exchanges will use household income and family size information based on taxpayer records to make an assistance determination.
Perform Reporting Activities	Business Object Enterprise	The IRS will use data for reporting purposes.

Source: Draft CDR Business System Report dated June 27, 2014.

The objective of this audit was to determine whether the IRS was adequately managing systems development risks for CDR 2.0, which is one of the core ACA systems. Data gathered and our audit steps focused on designated control points and other ongoing activities for the CDR 2.0 under ACA 4.0.

This review was performed at the IT ACA Program Management Office in Lanham, Maryland, during the period January through December 2014. 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.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Results of Review

Risks Could Not Be Effectively Mitigated by Testing Processes Planned for the Coverage Data Repository

The IRS Enterprise Life Cycle framework provides direction, processes, tools, and assets necessary to accomplish business change in a consistent and repeatable manner and helps ensure project success by reducing risk and ensuring compliance with applicable standards. According to the Enterprise Life Cycle, systems development and testing should be completed, to help ensure functionality, before a system is deployed into production.

Further, appropriate testing controls are critical to ensure that costly software and other changes are avoided after a system is deployed. The IRS IT ACA Implementation and Testing organization has the responsibility to ensure that the requirements and design for all ACA systems, including the CDR, have been adequately tested and operate as intended. This organization performed several types of testing for CDR 2.0 to determine whether the system would function as designed and meet the IRS's objectives for ACA 4.0.

- CDR 2.0 Project-Level Test. To verify the requirements and design for the CDR 2.0 system prior to ACA 4.0 release-level testing.
- ACA 4.0 Release-Level Test. A functional integration test responsible for verifying the interoperability of the ACA 4.0 systems, which includes the CDR and the Information Sharing and Reporting system, prior to CMS-IRS interagency testing.
- ACA 4.0 Interagency Test With the HHS Data Services Hub. A communication and functional integration test responsible for validating interoperability between the IRS and the CMS.
- ACA 4.0 Interagency Test With the Exchanges. To test transmission of the EPD from the Exchanges to the IRS, including data format and validation of file content via the HHS Data Services Hub.

Figure 5 provides the test types, test start dates, and test end dates for CDR-related testing.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Figure 5: Test Types, Test Start Dates, and Test End Dates for CDR 2.0 Testing

Test Type	Test Start Date	Test End Date
CDR 2.0 Project-Level System Test	10/23/2012	04/23/2014
ACA 4.0 Release-Level Test	04/07/2014	09/24/2014
ACA 4.0 Interagency Test With the HHS Data Services Hub	03/31/2014	09/30/2014
ACA 4.0 Interagency Test With the Exchanges (Federal Exchange, State Partnership Exchanges, and State Exchanges)	09/23/2014	Continuing through December 2014

Source: ACA 4.0 Consolidated Project-Level End of Test Completion Report dated August 15, 2014; ACA 4.0 Draft Release-Level Test End of Test Completion Report dated October 9, 2014; Implementation and Testing Organization's responses to a TIGTA questionnaire dated October 14, 2014; ACA 4.0 Draft Interagency Test End of Test Completion Report dated November 6, 2014; Implementation and Testing Organization's ACA 4.0 Interagency Test Weekly Briefing dated September 26, 2014; and Change Request Number ACA197 dated July 9, 2014.

The following sections discuss our review of the IRS's testing approach and results for interagency, release-level, and project-level testing.

Planned interagency testing with the Federal and State Exchanges has not been completed

The IRS's plans for ACA 4.0 to receive and store the EPD from the Exchanges to support the 2015 Filing Season. Starting with ACA 5.0, the IRS plans to use the EPD in at-filing and post-filing compliance activities to reliably verify Premium Tax Credit claims on individual income tax returns. The purpose of ACA 4.0/CDR 2.0 interagency testing with the Exchanges is to test end-to-end transmission of the EPD from the Exchanges via the HHS Data Services Hub to the IRS, including data format and validation of file content. The EPD includes sensitive taxpayer data for individuals who obtained health care coverage through the Exchanges. See Figures 1, 2, 3, and 4 for additional information on ACA releases, the EPD, and CDR 2.0 business processes and functionality.

The CMS and the IRS jointly developed a test plan that outlines the interagency testing activities for testing with the various Exchanges. The IRS completed the ACA 4.0 Interagency Test with the HHS Data Services Hub. However, interagency testing with the Exchanges was delayed and not completed before ACA 4.0/CDR 2.0 was deployed into production on September 30, 2014. Further, our review found that the IRS has extended this critical testing through December 2014 in an effort to allow the Exchanges to test transmission, data format, and validation of EPD file content. Specifically, on September 18, 2014, the IRS Chief Technology Officer approved a risk-based decision to continue interagency testing with the Exchanges through December 2014,



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

as requested by the CMS. During a September 24, 2014, meeting, the IT ACA executives explained that the IRS is concerned that interagency testing with the Exchanges was delayed and not completed before ACA 4.0 was deployed into production. The ACA Program Governance Board granted its unconditional approval to deploy ACA 4.0 on September 30, 2014. The IRS explained that the Program Governance Board granted its approval based on system readiness demonstrated during the ACA 4.0 release-level and partially completed interagency testing.

The IRS IT ACA executives also explained that although they were ready to conduct and complete interagency testing with the Exchanges before ACA 4.0/CDR 2.0 was deployed, the Exchanges were not ready to complete the planned testing at that time. They stated specifically that interagency testing with the Exchanges was delayed and extended to run through December 2014 due to the following two internal testing challenges for the CMS:

- The Federal Exchange application.
- Communication between the Exchanges and the HHS Data Services Hub.

To mitigate the IRS's risks resulting from incomplete interagency testing with the Exchanges, the IRS informed TIGTA that it executed simulated Exchange testing. This process involved replicating an EPD file with test data that the IRS anticipated would be provided from the Exchanges. The test data file was run through the ACA 4.0 systems, including the CDR and the Information Sharing and Reporting, prior to ACA 4.0 being deployed into production to make sure that the systems worked as intended.

ACA executives also informed TIGTA that the IRS completed release-level testing for its internal ACA 4.0 systems, including CDR 2.0, and completed interagency testing with the HHS Data Services Hub before ACA 4.0 was deployed into production. Based on this testing, they believe that the ACA 4.0 systems can successfully receive and process the EPD from the Exchanges as needed. They further explained that the purpose of testing with the Exchanges was to help the CMS and the States validate whether their Exchange systems could successfully send the EPD to the IRS and not to validate whether the IRS's ACA 4.0 systems functioned correctly. ACA executives stated that if an Exchange sends EPD data with errors, the IRS will flag the errors and send error codes back to the Exchange so it can correct the data.

As of November 21, 2014, the IRS had only received and loaded into the CDR the EPD from three States. Subsequent to our fieldwork, the IRS received additional data, but it still had not yet received all required EPD submissions from the Exchanges as of January 20, 2015, the start of the 2015 Filing Season. For example, the CMS did not plan to send approximately 1.7 million (40 percent) of the approximately 4.2 million Federal Exchange enrollment records to the IRS until mid-February. As of January 20, 2015, the IRS had received partial data for individuals in 35 of the 36 States participating in the Federal Exchange. In addition, six of the 15 State Exchanges had not provided enrollment data to the IRS as of January 20, 2015. The IRS anticipated receiving data from four of the six State Exchanges in mid-February. However, the



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

IRS has not received any indication from the remaining two State Exchanges as to when they will provide the required enrollment data.

In an e-mail alert correspondence to the IRS dated December 8, 2014, TIGTA recommended that the “IRS revise processes and procedures to freeze the portion of the refund attributed to the Premium Tax Credit when matches to both Forms 1095-A⁵ and EPD data do not confirm the individual purchased insurance through an Exchange. At a minimum, these processes should ensure the taxpayer purchased insurance from an Exchange before the Premium Tax Credit claim is paid.” The IRS responded that, “To the extent that information does not match and we are unable to resolve, we will be using existing pre-refund capabilities to freeze refunds to prevent erroneous refunds.”

Recommendation

Recommendation 1: The Chief Technology Officer should ensure that interagency testing with the Exchanges is completed and that all testing objectives for the CDR system have been met.

Management’s Response: The IRS disagreed with this recommendation. The Chief Technology Officer stated that the CDR system was fully tested prior to being deployed into production and that the IRS had extended interagency testing to help the Exchanges validate their systems. The CDR test objectives were not dependent on testing with the Exchanges, and the CDR testing objectives were met when the IRS successfully received the EPD from the HHS Data Services Hub and returned appropriate responses.

Office of Audit Comment: The IRS completed release-level testing for its internal ACA 4.0 systems, including CDR 2.0, and completed the first part of the ACA 4.0 Interagency Test with the HHS Data Services Hub. However, the IRS did not fully complete interagency testing with the Exchanges before ACA 4.0/CDR 2.0 was deployed into production. It was critical to complete interagency testing with the Exchanges to verify whether the Exchanges could successfully transmit their monthly EPD data files to the IRS. Because interagency testing with the Exchanges had not been completed as of January 20, 2015, the IRS did not verify that all the Exchanges would be able to successfully transmit their EPD data to the IRS as needed. Delays in receiving the EPD from the Exchanges increase the risk of not detecting erroneous Premium Tax Credit claims on individual income tax returns.

⁵ Form 1095-A, *Health Insurance Marketplace Statement*.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Release-level testing was completed but not prior to initiating interagency testing with the CMS

The *CMS-IRS Interagency Test Plan* dated January 23, 2014, required the CMS and the IRS to complete independent testing of their respective systems prior to the start of CMS-IRS interagency testing. The IRS executed its internal ACA 4.0 release-level testing, which included CDR 2.0, and interagency testing with the HHS Data Services Hub at nearly the same time. Specifically, the IRS executed ACA 4.0 release-level testing from April 7, 2014, through September 24, 2014, while CMS-IRS interagency testing was executed from March 31, 2014, through September 30, 2014. However, this approach did not fully test and verify the IRS's internal ACA 4.0 release-level functionality prior to starting ACA 4.0 interagency testing with the HHS Data Services Hub. During our meetings with the ACA IT Implementation and Testing organization, the IRS agreed that the ACA 4.0 release-level tests should have been completed before the start of ACA 4.0 interagency testing with the HHS Data Services Hub.

The ACA IT Implementation and Testing organization explained that the ACA 4.0 release-level test schedule was affected due to delays with code delivery that both the IRS and the CMS were responsible for completing. According to the IRS's ACA 4.0 Release-Level End of Test Completion Report, the release-level test was delayed due to several factors, including the following:

- High testing defect rates.
- Late delivery of code.
- Insufficient wording of requirements.

The IT Implementation and Testing organization further explained that it took steps to mitigate the risks with conducting ACA 4.0 release-level and interagency testing simultaneously. Specifically, the IRS coordinated and prioritized release-level and interagency test cases. This added process was undertaken so that certain ACA 4.0 functionality was first tested during the internal IRS release-level test before the interagency test tested the same functionality.

Because the IRS did not fully complete its internal ACA 4.0 release-level tests before the start of interagency testing, as required by the *CMS-IRS Interagency Test Plan*, the IRS could not ensure that its internal ACA 4.0 systems were fully functioning as intended prior to starting CMS-IRS interagency testing. For example, the IRS did not know whether its CDR and Information Sharing and Reporting systems, which make up ACA 4.0, could successfully and properly work together as a complete ACA 4.0 release. This increases the risk that interagency testing between the IRS and the CMS may not have effectively determined whether planned functionality works as intended between the two agencies.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Recommendation

Recommendation 2: The Chief Technology Officer should ensure that future ACA projects, including the CDR, complete release-level testing and mitigate identified defects before starting interagency testing.

Management's Response: The IRS disagreed with this recommendation. The Chief Technology Officer stated that the IRS uses management discretion when determining if integration tests, such as release-level testing and interagency testing, must run sequentially, can overlap, or can run in parallel. The response stressed that plans are static and generally do not anticipate every challenge that could surface in testing. The process of continually assessing, planning, and prioritizing the test case inventory occurs dynamically as the test cycle unfolds. This dynamic model, according to the Chief Technology Officer, allows the IRS to ensure that all tests are completed prior to deploying the system into production. The Chief Technology Officer stated that without such flexibility, development, test, and deployment efforts would be severely hampered.

Office of Audit Comment: The *CMS-IRS Interagency Test Plan* documented test design and test management activities agreed upon by the CMS and the IRS. This plan required the CMS and the IRS to complete independent testing of their respective systems prior to the start of CMS-IRS interagency testing to ensure that the IRS's internal ACA 4.0 systems (CDR and Information Sharing and Reporting systems) were fully functioning as intended prior to CMS-IRS interagency testing. Although the IRS attempted to mitigate the risks of conducting release-level and interagency testing simultaneously, it is a huge and complex undertaking to continually assess, plan, and prioritize the test case inventory as the test cycle unfolds. This type of testing approach introduced risks, inefficiencies, and the likelihood that planned functionality for the CDR may not work as intended between the two agencies.

Project-level testing End of Sprint Checkpoint Reviews did not sufficiently demonstrate that CDR functionality will satisfy ACA business requirements

The IRS business owner for the CDR system is the ACA Program Office, whose mission is to support the administration of the ACA tax provisions by supporting high levels of voluntary compliance while protecting the tax system from fraud and other noncompliance. Beginning with Tax Year 2015, the ACA Program Office will rely on the EPD, which is stored and transmitted by the CDR, to systemically verify the accuracy of Premium Tax Credit claims.

Internal Revenue Manual (IRM) 2.16, *Enterprise Life Cycle Guidance*, dated April 2012, and IRS Information Technology Iterative Development and Testing Process Description, dated November 2011, describe the iterative process as an approach by which projects start with initial planning and end with deployment, using repeated cycles known as sprints that demonstrate subsets of development and testing. The sprints are a step-by-step build approach that leads to



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

the development of the entire system. The IRM states that the iterative process relies on the close involvement of business owners,⁶ who should be part of the project team⁷ and contribute throughout the project.

With the Iterative Path, each sprint typically lasts four to six weeks and can run sequentially or in parallel with another sprint. At the completion of each sprint, a process called an End of Sprint Checkpoint Review occurs to ensure adequate development of software. Specifically, a key purpose of the End of Sprint Checkpoint Review process is to demonstrate the system's functionality to the system's stakeholders. At this control point, stakeholders provide feedback and approvals to the developers regarding whether the tested functionality meets business objectives. One primary purpose of the End of Sprint Checkpoint Review is to demonstrate the CDR to the ACA Program Office.

CDR developers conducted a series of 16 End of Sprint Checkpoint Reviews over a period of 15 months, beginning October 2012 and ending May 2014. However, our review found that developers only demonstrated the developed functionality during two of the 16 sprints. For the remaining 14 sprints, there were not actual demonstrations of the developed functionality but rather PowerPoint presentations in which CDR developers presented a report to the ACA Program Office summarizing the work conducted during the sprints. These reports contained technical terms and concepts such as data modeling, architecture spike, and product burn-up and burn-down charts that might not be understood by business personnel.

CDR IT organization management stated that it was difficult to demonstrate the system's functionality to the ACA Program Office at the End of Sprint Checkpoint Reviews because the CDR is a database without end users or an end-user interface. CDR IT organization management added that the database did not yet contain any EPD to allow a demonstration of the database's functionality. As such, the IRS believed that the End of Sprint Checkpoint Review reports were a clear and reliable depiction of the CDR's development that the ACA Program Office partners could reference in lieu of an actual demonstration.

However, the intent of the End of Sprint Checkpoint Review process is to provide an opportunity for developers to demonstrate the tested functionality to CDR business owners who then provide feedback and approval that the system satisfies its business needs. CDR developers did not demonstrate the system to the ACA Program Office at the end of each sprint. Without a demonstration of the system, the ACA Program Office could not reliably ascertain if the CDR functions being described at the End of Sprint Checkpoint Reviews satisfied its business needs. For instance, the ACA Program Office could not verify that the CDR contained the Income and Family Size Verification Response Codes table or that the CDR contained values for each data element.

⁶ The business owners are those who requested the IT organization to develop the system and who will use it upon completion to meet their objectives, goals, and measures.

⁷ The project team consists of the IRS business owner, the project manager, a business analyst, developers, and testers.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Recommendation

Recommendation 3: The Chief Technology Officer should verify whether CDR 2.0 functionality has been adequately demonstrated and is acceptable to ACA business owners.

Management's Response: The IRS disagreed with this recommendation. The Chief Technology Officer stated that the CDR only had two ACA 4.0 demonstrable products of interest to the business—the data model and the Extract, Transform, and Load process to load the data into the database. Both of these products were demonstrated to the business. The other sprints focused on nonfunctional requirements, which could not be demonstrated but were tested and the results included in the End of Sprint Checkpoint Reviews.

The CDR business owner drove a number of working sessions with the CMS and the IRS IT organization to define, at a detailed level, the format and packaging for the EPD data. Also, the business actively participated in a series of walkthrough presentations of the EPD data flow from intake to its use in at-filing compliance processing.

Office of Audit Comment: The IRS developed the *Iterative Development and Testing Process* document that describes key processes that are required by system development projects that elect to follow the Enterprise Life Cycle Iterative Path. Management review at key control points during software development is a required process. The primary purpose of End of Sprint Checkpoint Reviews is to have developers demonstrate the system's functionality to stakeholders and have stakeholders provide feedback regarding whether the tested functionality meets previously stated business requirements. It is critical for CDR developers to demonstrate to the ACA Program Office CDR's functionality during all sprints. While the IRS explained that the business actively participated in a series of walkthrough presentations of the EPD data flow from intake to its use in at-filing compliance processing, this functionality is part of ACA 5.0, which was not included in the scope of this audit.

Project-level testing did not maintain complete records of business stakeholder participation in the CDR development process

The End of Sprint Checkpoint Review process provides multiple opportunities during the iterative systems development process for business stakeholders to provide feedback. Feedback includes approval for developers to proceed to the next sprint once business owners accept the tested piece of system functionality and agree that it will meet their business needs. Business owners are generally part of the project team. IRM guidance states that the End of Sprint Checkpoint Review process should document attendance rosters, meeting minutes, feedback from the stakeholders, a detailed development plan to address feedback, and lessons learned.

CDR IT organization management stated that the members of the ACA Program Office were part of the CDR Project team and worked in close proximity with the developers throughout the



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

sprints. Although the ACA Program Office's concerns and feedback were not documented, CDR IT organization management indicated they were generally addressed during sprint testing. However, meeting minutes to verify the ACA Program Office's involvement and participation were not available. The IRS considers the End of Sprint Checkpoint Review report as a record of the meeting.

Accordingly, CDR IT organization management did not provide sufficient evidence to support adequate business stakeholder involvement and participation throughout the sprints and in the End of Sprint Checkpoint Review meetings. Although CDR IT organization management provided End of Sprint Checkpoint Review attendance rosters, the IRS did not maintain the required sprint meeting minutes or documented stakeholder feedback to verify adequate ACA Program Office participation. As such, the ACA Program Office could not completely verify that the CDR was capable of receiving the EPD.

Without sufficient documentation as evidence that the ACA Program Office was sufficiently involved throughout the CDR sprints and during the End of Sprint Checkpoint Review process, there is limited assurance that the End of Sprint Checkpoint Review process is working as intended. Additionally, without adequate participation from the ACA Program Office throughout the sprints and at the End of Sprint Checkpoint Review, and documentation to support this participation, the End of Sprint Checkpoint Review process cannot be relied upon as an effective management control to ensure that the CDR will satisfy stated business requirements.

Recommendation

Recommendation 4: The Chief Technology Officer should ensure that sufficient evidence is maintained to verify adequate business owner participation and acceptance of CDR functionality.

Management's Response: The IRS acknowledged this recommendation and expressed concern that it is based on an IRM that was not in effect at the time of the ACA 4.0 development sprints. The Chief Technology Officer stated that the CDR Project followed the Enterprise Life Cycle Iterative Path guidance that was in place at the time and gathered business partner signatures on the End of Sprint Checkpoint Reviews as evidence of their concurrence.

Office of Audit Comment: The finding and recommendation are based on IRM 2.16.1, *Enterprise Life Cycle*, dated April 2012, and an analysis of the CDR 2.0 project-level test that included the End of Sprint Checkpoint Reviews started on October 23, 2012, and ended on April 23, 2014. TIGTA maintains that it is important for the Chief Technology Officer to address this recommendation for future CDR systems development to ensure that sufficient evidence is maintained to verify adequate business stakeholder involvement and participation throughout the sprints and in the End of Sprint Checkpoint Review meetings.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Improved Controls Are Needed to Ensure That Only Approved Applications Are Deployed Into the Internal Revenue Service's Production Environment

IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, dated December 2013, provides policies and guidance to be used by IRS organizations to carry out their information systems security responsibilities. The IRM requires that a senior-level executive or manager be appointed as the authorizing official for each information system. This authorizing official assumes responsibility for and is accountable for security risks associated with the operation and use of the designated organizational information systems. The authorizing official approves the information system for processing before it is deployed into production operations. In the IRS, this authorization is accomplished by issuance of an Authority to Operate memorandum.

The authorizing official for the ACA Information System Release 4.0 issued the Authority to Operate memorandum on September 8, 2014, before CDR 2.0 was deployed into the IRS production environment on September 30, 2014. *****2*****
*****2*****. The Authority to Operate for ACA 4.0 states that "...for the Primary General Support System for which this application will run must also review the security risks associated with this application and will need to concur with this Authority to Operate to allow this application to operate in the targeted General Support System environment prior to it being released into production. That concurrence will be received via separate Authority to Operate memo for the targeted General Support System." However, our review identified that the authorizing official for the *****2***** (General Support System 41) did not issue the Authority to Operate memorandum before the CDR was deployed into the IRS production environment on September 30, 2014. The authorizing official approved the Authority to Operate General Support System 41 memorandum on November 17, 2014, almost two months after the CDR system was deployed. IRS officials were unable to explain the cause for not issuing the General Support System 41 Authority to Operate memorandum authorizing operation of the CDR system before it was deployed into the IRS production environment.

Since the IRS deployed the CDR system with known security risks, the IRS subsequently developed a Plan of Action and Milestones to implement corrective actions. While CDR officials have developed mitigation plans for the security risks as required by IRM guidelines, the needed corrective measures will not be implemented until September 2015. *****2*****
*****2*****⁸ *****;

- *****2*****⁹ *****2*****
*****2*****

⁸ Our audit scope did not include a detailed analysis of the security weaknesses the IRS has identified for the CDR.

⁹ IRM 10.8.6.3.13.7, dated September 30, 2014, 10.8.6 Information Technology (IT) Security, Secure Application Development defines mobile code as follows: National Institute of Standards and Technology Special Publication 800-28 Rev 2, Guidelines on Active Content and Mobile Content, recognizes how the Department of Defense



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

*****2*****
*****2*****.

- *****2*****
*****2*****
*****2*****
*****2*****
*****2*****
*****2*****.
- *****2*****
*****2*****
*****2*****.

Recommendation

Recommendation 5: The Chief Technology Officer should ensure that authorizing officials evaluate and accept CDR risks prior to deployment.

Management's Response: The IRS agreed with this recommendation. IRS management stated that they updated applicable security operating procedures and templates reflecting explicit risk acceptance from the CDR authorizing official in addition to updating the risk notification process to enable security staffs and authorizing officials to recognize risks prior to deployment.

The Coverage Data Repository Audit Plan Was Not Implemented to Support the Internal Revenue Service's Unauthorized Access to Taxpayers' Records Program

The willful unauthorized access or inspection of taxpayer records is a crime, punishable upon conviction, by fines, imprisonment, and termination of employment. To protect sensitive tax return information from unauthorized access and to implement provisions of the Taxpayer Browsing Protection Act of 1997,¹⁰ the IRS has established the Unauthorized Access (UNAX), Attempted Access, or Inspection of Taxpayers' Records program (UNAX program). The UNAX program requires the implementation of controls to restrict and monitor access to

delineates three categories of technology based on increasing associated risk: Category 1 – This is the most dangerous category, and it involves technologies having broad functionality and unmediated access to the services and resources of a computing platform. The two subcategories of Category 1 mobile code technologies include 1A and 1X. Category 2 – Involves technologies having full functionality, but mediated or controlled access to the services and resources of a computing platform. Category 3 – Involves technologies having limited functionality, with no capability for unmediated access to the services and resources of a computing platform.

¹⁰ 26 U.S.C. §§ 7213, 7213A, and 7431.



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

taxpayer data across the entire IRS enterprise. The CDR database is described as the IRS's sole authoritative source of all ACA data for health care-related functions and services. Specifically, the CDR should include access and audit trail controls necessary to enforce the UNAX program for the following type of Personally Identifiable Information: name, SSN, Taxpayer Identification Number, address, date of birth, salary information, date of death, and income level.

The solution architecture for the CDR relies on multiple system components to deliver needed business functionality. As dictated by the solution architecture, the completion of the CDR Application Audit Plan depends on the completion of the following system component audit plans. *****2*****.

- *****2*****.
- *****2*****.
- *****2*****.
- *****2*****.
- *****2*****.
- *****2*****.

The IRS's policies and procedures provide guidance for capturing, storing, transmitting, reviewing, and retaining audit trails. These policies and procedures require that audit trails be sufficient in detail to facilitate the reconstruction of events if unauthorized activity or a malfunction occurs or is suspected of occurring on enterprise computing assets. Figure 6 provides an overview of the CDR solution architecture and the various system components, including data exchange paths, along with the IRS security perimeter and portal for ACA processes and services.

[illegible]

The IRS *Information Technology (IT) Security, Audit Logging Security Standards*, provides that detailed audit implementations and approved minimum auditable events shall be documented in an approved audit plan and provided during initial authorization activities as required by the Enterprise Life Cycle when exiting the systems development milestone, Milestone 4b.

Page 21



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

and applications to develop audit plans and readies audit tools to collect and store information system events.

Audit plans must be developed for all deployed IRS systems and applications. The audit plans should:

- Detail the purpose and objectives of the audit plan.
- Detail the scope of the audit.
- Describe the type of information to be audited.
- Describe when and how much time is available to review audit logs.
- Detail the resources available for collecting and storing audit logs.
- Describe the types of auditable events that will be collected.
- Provide technology-specific implementation guidelines and tool-specific parameters requirements.
- Document the required retention period for online audit logs.
- Document the required retention period for archived audit logs.
- Identify whether applications contain taxpayer data.

IRS security policy also requires that the IRS:

- View security risk–related considerations for individual information systems from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization.
- Manage risks for individual information systems consistently across the enterprise, reflect the IRS’s risk tolerance, and consider risks for individual systems, along with other organizational risks.
- Share security risk-related information among the authorizing officials and other senior management/executive officials enterprise-wide.
- Cooperate and collaborate among the authorizing officials to include authorization actions requiring shared responsibility.

The CDR Release 2.0 project exited Milestone 4b in September 2014 and has been deployed. Our review found that the required CDR Application Audit Plan had not been approved as of December 2014. Further, the IRS has not yet initiated testing of CDR controls planned to support UNAX policies. Testing of these controls is dependent on completion and approval of the CDR Application Audit Plan including CDR audit requirements and UNAX test scripts.



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

Our analysis identified incomplete program planning and scheduling across the authorizing officials and parties responsible for the CDR. Specifically, for the CDR to support the IRS's UNAX policies, management, operational, and technical controls need to be planned, developed, approved, and tested during key activities. This includes during application development, system component implementation and integration, approval and updates for the Application Audit Plan, and approval and updates for the CDR system component audit plans. The IRS stated that the CDR Application Audit Plan has not yet been completed due to a lack of funding and resources.

Once the CDR Application Audit Plan has been implemented successfully, audit trails must provide specific information on events associated with access to sensitive taxpayer data, including when the events occurred and who or what caused the events. This information will allow the IRS to reconstruct events, monitor compliance with security policies, identify malicious activity or intrusion, and analyze user and system activity. As such, the CDR Application Audit Plan is the key planning document to meet the IRS's goals to comply with audit trail standards. Without implementation of an approved CDR Application Audit Plan, the IRS will be unable to capture all auditable events and related data elements that are required to effectively support UNAX investigations, identify noncompliant activity, and hold employees accountable for UNAX policies.

Recommendation

Recommendation 6: The Chief Technology Officer should ensure that the CDR Application Audit Plan and related system component audit plans are completed, approved, sufficiently tested, and implemented.

Management's Response: The IRS agreed with this recommendation. IRS management stated that they will ensure that the CDR Application Audit Plan and related system component audit plans are completed, approved, sufficiently tested, and implemented.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Appendix I

Detailed Objective, Scope, and Methodology

The overall audit objective was to determine how systems development risks for the CDR Project were being mitigated and whether established business and information technology requirements were being met. To accomplish the objective, we performed tests related to the following areas:

- I. Project Management Controls – Determined the effectiveness of project management controls over the Enterprise Life Cycle artifacts.
 - A. Reviewed key artifacts including the CDR Project Charter, the CDR Project Tailoring Plan, the CDR Project Management Plan, the Milestone Readiness Review, the Milestone Exit Review, and the End of Sprint Checkpoint Review reports.
 1. Evaluated whether End of Sprint Checkpoint Review reports were approved by the appropriate stakeholders as evidence that stakeholders agreed that proper functionality was developed and tested for each sprint.¹
- II. Systems Testing
 - A. Release-Level Testing – The IRS explained that release-level testing was extended to September 15, 2014, due to additional code deliveries. Some release-level testing and interagency testing activities are being conducted simultaneously.
 1. Determined if conducting release-level testing and interagency testing activities simultaneously is permissible. If not, we determined how this could affect ACA 4.0/CDR 2.0.
 - B. Interagency Testing – According to the IT ACA Program Management Office Briefing to the Chief Technology Officer dated March 7, 2014, the IRS envisioned that it is desirable to extend the current interagency testing model to include engagement with the State Exchanges for EPD reporting. We determined whether the plan include testing with the State Exchanges for EPD reporting.
 1. Inquired and documented the risks to the IRS if this testing was not conducted.
- III. Security Testing – Determined whether the IRS had taken sufficient and appropriate actions to mitigate identified ACA 4.0/CDR 2.0 security risks, to conduct and resolve testing risks related to ACA 4.0/CDR 2.0 security requirements, and to implement audit

¹ See Appendix VII for a glossary of terms.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

trail/UNAX controls in accordance with established IRS/National Institute of Standards and Technology policy.

- A. Reviewed security guidelines, including IRM 10.8.1 (December 2013) and National Institute of Standards and Technology Special Publication 800-53 Revision 4 (April 2013) which were in existence during the October 2013 ACA 3.0 deployment date.
 - B. Reviewed the CDR Security Risk Assessment report to determine the key risks identified for the CDR. We ensured that mitigation actions were sufficient and complied with established National Institute of Standards and Technology and IRM security guidelines.
- IV. Audit Trails/UNAX – Assessed the adequacy of the IRS’s implementation of ACA CDR Audit Trails/UNAX controls.
- A. Evaluated the CDR’s audit trails/UNAX implementation by reviewing the CDR Application Audit Plan, audit trail capabilities, and audit trail test artifacts and test results.
- V. Fraud Detection – Determined what fraud mitigation controls will be in effect to detect ACA CDR-related fraud for the 2015 Filing Season.

Internal controls methodology

Internal controls relate to management’s plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined that the following internal controls were relevant to our audit objective: IRM and related IRS guidelines and the processes followed in the development of information technology projects using the Iterative Path as they apply to the ACA Program’s CDR Project. We evaluated these controls by conducting interviews with management and staff and reviewing relevant documentation. Documents reviewed include the CDR Project Management Plan, the CDR End of Sprint Checkpoint Reviews, the CDR Plan of Action and Milestones, the CDR Security Risk Assessment, and other documents that provided evidence of whether the IRS is adequately managing systems development risks for the CDR Project.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Gwendolyn McGowan, Director
Carol Taylor, Audit Manager
David Allen, Senior Auditor
Andrea Barnes, Senior Auditor
Wallace Sims, Senior Auditor
Rita Woody, Senior Auditor
Chinita Coates, Auditor
Hung Dam, Information Technology Specialist



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

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
Director, Affordable Care Act Office SE:ACA
Deputy Chief Information Officer for Operations OS:CTO
Director, Privacy, Governmental Liaison, and Disclosure OS:P
Associate Chief Information Officer, Affordable Care Act (PMO) OS:CTO:ACA
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:
 Deputy Commissioner for Services and Enforcement SE
 Director, Business Planning and Risk Management OS:CTO:SP:RM



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Appendix IV

Exchange Periodic Data Elements¹

****2****	*****2*****
*****2*****2	
*****2**** *****2****	*****2***** *****2*****.
*****2***** ***2*****	*****2***** *****2***** *****2*****.
*****2***** *****2***** *****2****	*****2***** *****2***** *****2*****.
****2*****	*****2***** *****2*****.
2**	*****2*****.
*****2*****	*****2***** *****2*****.
*****2***** *****2*****	*****2***** *****2*****.
*****2*****	*****2***** *****2*****.
*****2***** *****2****	*****2***** *****2*****.
*****2*****	*****2*****.

¹*****2*****
*****2*****.

²*****2*****.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

****2****	*****2*****
*****2*****2*****2	
*****2*****	*****2*****.
*****2***** *****2*****	*****2***** *****2*****.
*****2***** *****2*****	*****2***** *****2***** *****2*****.
*****2****	*****2*****.
*****2***** *****2*****	*****2*****.
*****2***** ***2*****	*****2*****.
*****2*****	*****2*****.
*****2***** *****2*****	*****2***** *****2*****.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Appendix V

*Coverage Data Repository 2.0
Systems Development and Testing Timeline*

Key Dates	Description
March 2010	President Obama signs the Health Care and Education Reconciliation Act of 2010 and the Patient Protection and Affordable Care Act. ¹
April 2012	IRS ACA Governance Board provides approval to launch CDR 2.0 and other ACA 4.0 projects.
October 2012	CDR 2.0 begins project-level functional testing for ACA 4.0.
October 2013	The IRS deploys ACA 3.0 and the CDR begins accepting requests for Income and Family Size Verification and Advance Premium Tax Credit determinations.
March 2014	ACA 4.0 begins interagency testing with the HHS Data Services Hub.
April 2014	The CDR ends project-level functional testing for ACA 4.0.
April 2014	The CDR begins release-level testing with other ACA 4.0 applications.
September 4, 2014	The IRS's Enterprise Life Cycle Office recommends the CDR for a conditional Milestone Exit Review for Milestone 4b. ²
September 8, 2014	The Business Director of the ACA Program Office signs off on the Authority to Operate memorandum giving permission for the ACA 4.0 system to operate in production.
September 12, 2014	The CDR begins limited interagency testing with the Exchanges. The CDR was originally scheduled to start this testing in March 2014 and end in August 2014.

¹ Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029. See Appendix VII for a glossary of terms.

² Milestone 4b is the Systems Development Phase of the IRS's Enterprise Life Cycle.



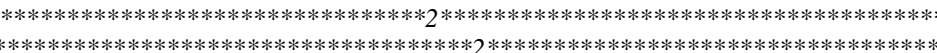
*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Key Dates	Description
September 17, 2014	The IRS ACA Governance Board approves ACA 4.0 to exit Milestone 4b.
September 18, 2014	The Chief Technology Officer makes a risk-based decision to extend interagency testing with the Exchanges beyond the September 30, 2014, deployment date until the end of December 2014.
September 23, 2014	The CDR begins interagency testing with the Exchanges. The CDR Project was originally scheduled to begin this testing in mid-July 2014.
September 24, 2014	The CDR ends ACA 4.0 release-level testing with other ACA 4.0 applications. ACA 4.0 release-level testing was originally scheduled to end at the end of June 2014.
September 26, 2014	The IRS ACA Governance Board approves ACA 4.0 to “go live.”
September 30, 2014	ACA 4.0 ends interagency testing with the HHS Data Services Hub that started in March 2014. This testing was originally scheduled to end at the end of August 2014.
September 30, 2014	The CDR goes into production and is ready to receive the EPD from the HHS Data Services Hub.
October 2014	The CDR begins receiving the EPD. At this point, the IRS had only received and loaded into the CDR the EPD from two State Exchanges.
November 2014	The CDR continues interagency testing with the Exchanges. At this point, the IRS had only received and loaded into the CDR the EPD from three State Exchanges.
December 2014	The CDR was scheduled to end interagency testing with the Exchanges.

Source: The IRS IT ACA Program Management Office.



Coverage Data Repository High-Level Logical System Architecture

Source: 2



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Appendix VII

Glossary of Terms

Term	Definition
Adjusted Gross Income	Gross income minus adjustments to income.
Advance Premium Tax Credit	The advance payment of the Premium Tax Credit allowed to an individual. It is paid to the issuer of a qualified health plan on a monthly basis.
Affordable Care Act	The comprehensive health care reform law enacted in March 2010 and subsequently amended. The law was enacted in two parts. The Patient Protection and Affordable Care Act ¹ was signed into law on March 23, 2010, and was amended by the Health Care and Education Reconciliation Act on March 30, 2010. The ACA refers to the final, amended version of the law.
Applicant	An individual who applies for enrollment in a qualified health plan offered through an Exchange.
Centers for Medicare and Medicaid Services	A division of the HHS, the CMS provides health coverage for 100 million people through Medicare, Medicaid, and the Children's Health Insurance Program.
Confidence Level Determination	A means of verifying that the required security controls have been implemented and can be achieved.
Consent Checking	A means of verifying that applicants authorize and consent to allow the IRS to share their personal information with other parties, including Federal and State agencies.
Data Services Hub	A tool that allows the CMS to interface and share ACA-related information with other agencies.
Department of Health and Human Services	The U.S. Government's principal agency for protecting the health of all Americans and providing essential human services.

¹ Pub. L. No. 111-148, 124 Stat. 119 (2010) (codified as amended in scattered sections of the U.S. Code), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029.



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

Term	Definition
Exchange	A new transparent and competitive insurance exchange where individuals and small businesses can buy affordable and qualified health benefit plans. Exchanges will offer a choice of health plans that meet certain benefits and cost standards.
Exchange Periodic Data	The data the IRS receives each month from the Exchanges. The EPD flows are cumulative, meaning each submission will contain data for each month from January up to and including the current month being submitted. See Appendix IV for the EPD elements.
Family Size	Relevant for purposes of computing the Premium Tax Credit, a taxpayer's family size equals the number of individuals for whom the taxpayer is allowed a deduction for the taxable year.
Federal Exchange	An Exchange developed by the Federal Government (the CMS) to assist States that have chosen not to build their own individual State marketplace.
HHS Data Services Hub	Provides a single point where the Exchanges may access data from different sources, primarily Federal agencies. The HHS Data Services Hub does not store data; rather, it acts as a conduit for the Exchanges to access the data from where they are originally stored.
Household Income	Relevant for purposes of determining eligibility for the Premium Tax Credit under Internal Revenue Code Section 36B and the individual shared responsibility payment under Internal Revenue Code Section 5000A. The term "household income" refers to any taxpayer with an income.
Income and Family Size Verification	A tool used to verify income and family size for individuals requesting eligibility for an Advance Premium Tax Credit for health insurance.
Information Sharing and Reporting	The Information Sharing and Reporting Project is responsible for facilitating the exchange of ACA data between IRS systems and the Exchanges. The Information Sharing and Reporting system performs consistency checks on the EPD before transmitting it to the CDR.
Iterative Systems Development Path	An adaptive development approach in which projects start with initial planning and end with deployment, with repeated cycles of requirement discovery, development, and testing in between. It is a more flexible and adaptable process than traditional sequential development approaches.
Personally Identifiable Information	Any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, and mother's maiden name.
Premium Tax Credit	A refundable tax credit to help taxpayers and families afford health insurance coverage purchased through an Exchange.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Term	Definition
Release	A specific edition of software.
Second Lowest Cost Silver Plan	Plans in the Exchanges are primarily separated into four health plan categories (Bronze, Silver, Gold, or Platinum) based on the percentage the plan pays of the average overall cost of providing essential health benefits to members. The Premium Tax Credit is calculated using the Second Lowest Cost Silver Plan, regardless of what plan the taxpayer ultimately selects.
Shared Secret Validation	A process whereby the IRS validates identity using IRS internal tax data before completing a service request from Federal or State agencies that discloses Federal tax information. The data that are used as a shared secret will be available in the CDR after the transfer of tax records.
Sprint	A process that develops a piece of functionality of the system with repeated cycles of requirements discovery, planning, design, development, and testing. ACA projects conduct a series of "sprints," either sequentially or even in parallel, within each release. The goal of each sprint is to get a subset of the project's functionality.
State Exchange	An Exchange fully operated by the individual State.
State Partnership Exchanges	A hybrid model in which a State makes key decisions and works with the HHS to tailor the operation of the Federal Exchange to meet the local needs and market conditions in the State.



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Appendix VIII

Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

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

APR 14 2015

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

Terence V. Milholland
Chief Technology Officer

SUBJECT:

Affordable Care Act Coverage Data Repository:
Risks with System Development and Deployment
Audit #201420310 (e-trak #2015-65370)

Thank you for the opportunity to review your draft audit report and to discuss earlier draft report observations with the audit team. We believe we achieved the intended result of the audit team's recommendations and fully demonstrated this to the audit team during the course of their field work. Two of the recommendations required minor corrective actions on our part; one was completed in February 2015 and the other is on plan to be completed this calendar year.

The IRS has a focused role in implementing several provisions of the ACA legislation and has successfully delivered several major ACA Program Releases. The IRS developed the Coverage Data Repository (CDR) as the IRS's authoritative source of data regarding ACA coverage-related functions and services and it is important to note that no personal health information or healthcare data is collected or stored by the IRS. The CDR is an integral component of the ACA Program. Our first implementation supported the initial rollout of the insurance exchange open enrollment in 2013 and has been operating continuously, without fail. Certainly, many factors contribute to the success of an IT project, and the areas highlighted in your report are key contributors; testing, business customer engagement, and security and audit trail controls.

We place a high degree of emphasis on the importance and the value of testing as was demonstrated during the course of this audit. The IRS developed a robust strategy to ensure the IRS systems were fully tested and concluded all required tests prior to Go-Live. The strategy included a dynamic process of continually assessing, planning, and prioritizing the test case inventory as the test cycle unfolded. Management must often use discretion in determining where integration tests, such as release level testing and interagency testing, must run sequentially, may overlap, or run in parallel. It is this dynamic model which allowed us to ensure all tests of the IRS systems were completed prior to putting them into production. Without this flexibility, development, test and deployment efforts would have been severely hampered.

The IRS agreed to expand Interagency testing to those Exchanges requesting it, as a means to assist the Exchanges in validating their systems. These tests began prior to the IRS Go-Live date and continued post Go-Live based upon an approved CMS change



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

2

request to do so. None of this testing was required to determine IRS systems readiness for Go-Live.

Also highlighted in your report is the value derived from including the business owners in project key milestones to ensure that system functionality has been adequately demonstrated and found acceptable. Through the ACA Program, the IRS has made great strides in the iterative development path and has a very strong IT-to-Business relationship. This was made known to the audit team both in the form of documentation and in interviews with the business customers. The CDR team conducted numerous reviews and the business customer was present at each. The CDR team had two demonstrable products of interest to the business customer; the data model, and the process used to load the data into the data base implementation of the model. Both of these products were demonstrated to the business customer.

As further evidence of the level of business engagement, the CDR business owner led a number of working sessions with CMS and IRS IT to define, at a detailed level, the XML format and packaging for the EPD data. Additionally, the business customer actively participated in a series of walk-throughs of the EPD data flow from intake to its use in at-filing processing. The final presentation, attendance records, and minutes of these walk-throughs were provided to the TIGTA audit team but were not referenced in this report.

We are committed to continuously improving the IRS information technology systems and processes. We value your continued support and the assistance and guidance your team provides. Our corrective action plan for the recommendations for which we are in agreement is attached. If you have any questions, please contact me at (240) 613-9373, or a member of your staff may contact Perry Robinett, Program Oversight Coordination Manager, at (240) 613-3780.

Attachment



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

Attachment

Draft Audit Report - Affordable Care Act Coverage Data Repository: Risks with System Development and Deployment (Audit # 201420310) (e-trak# 2015-65370)

RECOMMENDATION #1: The Chief Technology Officer should ensure that interagency testing with the Exchanges is completed and that all testing objectives for the CDR system have been met.

CORRECTIVE ACTION #1: We disagree with this recommendation. The CDR system was fully tested prior to being put into production. The focus of interagency testing was to ensure that the IRS could successfully receive EPD from the CMS Data Services Hub and return appropriate responses back to the Hub. CDR test objectives were not dependent on testing with the Exchanges. The IRS extended interagency testing to include testing with the State and Federal exchanges as a means to help the Exchanges validate their systems. CDR testing objectives were met when we successfully received EPD from the Hub and returned an appropriate response.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #2: The Chief Technology Officer should ensure that future ACA projects, including the CDR, complete release-level testing and mitigate identified defects before starting interagency testing.

CORRECTIVE ACTION #2: We disagree with this recommendation. IRS uses management discretion when determining where integration tests, such as release level testing and interagency testing, must run sequentially, may overlap, or can run in parallel. Plans are static and generally do not anticipate every challenge that could surface in testing. The process of continually assessing, planning, and prioritizing the test case inventory occurs dynamically as the test cycle unfolds. It is this dynamic model which allows us to ensure all tests are completed prior to putting the system into production. Without this flexibility, development, test and deployment efforts would be severely hampered.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #3: The Chief Technology Officer should verify whether CDR 2.0 functionality has been adequately demonstrated and is acceptable to ACA business owners.



Affordable Care Act Coverage Data Repository: Risks With Systems Development and Deployment

Attachment

Draft Audit Report - Affordable Care Act Coverage Data Repository: Risks with System Development and Deployment (Audit # 201420310) (e-trak# 2015-65370)

CORRECTIVE ACTION #3: We disagree with this recommendation. The CDR team conducted a series of 21 Sprints including 5 design sprints with active business participation, 13 development sprints, and 3 Integration Sprints in support of Release Level Testing. TIGTA reviewed the End of Sprint Checkpoint Reviews for the 13 development sprints and the 3 Integration Sprints. In ACA 4.0 CDR only had two demonstrable products of interest to the business, the data model, and the ETL process to load the data into the data base implementation of the model. Both of these products were demonstrated to the business. The other sprints focused on Non-Functional requirements which cannot be demonstrated, but were tested and the results included in the End of Sprint Checkpoint Reviews.

Additionally, but not mentioned in TIGTA's report, the CDR Business Owner drove a number of working sessions with CMS and IRS IT to define, at a detailed level, the XML format and packaging for the EPD data. Also, the business actively participated in a series of walk-throughs of the EPD data flow from intake to its use in At-Filing compliance processing. The final presentation, attendance records and minutes of these walk-throughs were provided to TIGTA but not referenced in this report.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #4: The Chief Technology Officer should ensure that sufficient evidence is maintained to verify adequate business owner participation and acceptance of CDR functionality.

CORRECTIVE ACTION #4: The IRS acknowledges this recommendation. However, this recommendation is based on a reference to an IRM that was not in effect at the time of the ACA 4.0 development Sprints. The CDR project followed the ELC Iterative Guidance that was in place at the time and gathered Business partner signatures on the End of Sprint Checkpoint Reviews as evidence of their concurrence. During the course of the audit, the audit team interviewed several representatives of the owning business organization and were informed of their active participation. As is our normal custom, the IRS will follow applicable guidance during the project life cycle.

IMPLEMENTATION DATE: Completed, May 2014

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, ACAPMO

CORRECTIVE ACTION MONITORING PLAN: N/A



*Affordable Care Act Coverage Data Repository:
Risks With Systems Development and Deployment*

Attachment

Draft Audit Report - Affordable Care Act Coverage Data Repository: Risks with System Development and Deployment (Audit # 201420310) (e-trak# 2015-65370)

RECOMMENDATION #5: The Chief Technology Office should ensure that authorizing officials evaluate and accept CDR risks prior to deployment.

CORRECTIVE ACTION #5: The IRS agrees with this recommendation and has updated accordingly applicable security operating procedures and templates reflecting explicit risk acceptance from the CDR Authorizing Official (AO), in addition to updating the risk notification process to enable GSS security staffs and AOs to recognize risks prior to deployment.

IMPLEMENTATION DATE: Completed, February 2015

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: N/A

RECOMMENDATION #6: The Chief Technology Officer should ensure that the CDR Application Audit Plan and related system component audit plans are completed, approved, sufficiently tested, and implemented.

CORRECTIVE ACTION #6: The IRS agrees and will ensure that the CDR Application Audit Plan and related system component Audit Plans are completed, approved, sufficiently tested, and implemented.

IMPLEMENTATION DATE: September 15, 2015

RESPONSIBLE OFFICIAL: The Associate Chief Information Officer, Cybersecurity

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