TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

*Improved Controls Are Needed to
Ensure That Corrective Actions for
Reported Information Technology
Weaknesses Are Documented and
Fully Implemented Prior to Closure*

September 19, 2018

Reference Number: 2018-20-063

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

IMPROVED CONTROLS ARE NEEDED TO ENSURE THAT CORRECTIVE ACTIONS FOR REPORTED INFORMATION TECHNOLOGY WEAKNESSES ARE DOCUMENTED AND FULLY IMPLEMENTED PRIOR TO CLOSURE

Highlights

Final Report issued on September 19, 2018

Highlights of Reference Number: 2018-20-063 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

Internal controls are a major part of managing an organization and provide reasonable assurance that organizational objectives are being achieved. Internal controls protect assets, detect errors, and prevent fraud. The IRS is increasingly vulnerable to negative impacts from not addressing previously reported and agreed-to weaknesses in its controls. In addition, by not addressing the weaknesses and fully implementing the Planned Corrective Actions, realization of program benefits related to IRS management of taxpayer data and organizational improvements could be negatively affected.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether closed corrective actions reported by the IRS's Information Technology organization from prior TIGTA audits have been adequately documented, appropriately approved, and fully implemented. Specifically, TIGTA focused the review on a judgmental sample of closed corrective actions involving IRS systems development and operations recommendations.

WHAT TIGTA FOUND

The Chief Financial Officer's Office of Audit Coordination supports the day-to-day internal control program and is responsible for managing the Department of the Treasury's Joint Audit Management Enterprise System related activities for the IRS.

While approving officials and the Office of Audit Coordination approved each sampled corrective action closure, TIGTA determined that in two instances the IRS did not fully describe in the supporting documentation the specific actions taken to close the Planned Corrective Actions. In addition, the IRS did not upload sufficient supporting documentation into the Joint Audit Management Enterprise System to support proper closure for six sampled Planned Corrective Actions. TIGTA also found that four (20 percent) of 20 judgmentally sampled closed Planned Corrective Actions to address reported control weaknesses from prior TIGTA audit reports were not fully implemented.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Financial Officer ensure that complete descriptions of the specific actions taken to close Planned Corrective Actions are documented and that sufficient supporting documentation is uploaded to the Joint Audit Management Enterprise System to support closure of Planned Corrective Actions. In addition, TIGTA recommended that the Chief Information Officer ensure that the prematurely closed Planned Corrective Actions are reopened and monitored until fully implemented.

The IRS agreed with all recommendations. The IRS plans to review and update as necessary existing policy to ensure that program owners are required to completely document actions taken to satisfy Planned Corrective Action closure requirements; continue conducting reviews throughout the year of a sample of closed Planned Corrective Actions to ensure that the IRS meets documentation requirements; and reopen and monitor until fully implemented the prematurely closed Planned Corrective Actions.

September 19, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improved Controls Are Needed to Ensure That
Corrective Actions for Reported Information Technology Weaknesses
Are Documented and Fully Implemented Prior to Closure
(Audit # 201820013)

This report presents the results of our review to determine whether closed corrective actions reported by the Internal Revenue Service's Information Technology organization from prior Treasury Inspector General for Tax Administration audits have been adequately documented, appropriately approved, and fully implemented. Specifically, we focused our review on a judgmental sample of closed corrective actions involving Internal Revenue Service systems development and operations recommendations. This review is included in our Fiscal Year 2018 Annual Audit Plan and addresses the major management challenge of Achieving Program Efficiencies and Cost Savings.

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

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

Table of Contents

Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
CTO	Chief Technology Officer
ERS	Error Resolution System
GAO	Government Accountability Office
IRS	Internal Revenue Service
JAMES	Joint Audit Management Enterprise System
PCA	Planned Corrective Action
PII	Personally Identifiable Information
SBU	Sensitive But Unclassified
TIGTA	Treasury Inspector General for Tax Administration

Background

According to Internal Revenue Manual[1] 1.4.30, *Resource Guide for Managers, Monitoring Internal Control Planned Corrective Actions*, dated October 16, 2015, internal controls are a major part of managing an organization. Internal controls are comprised of the plans, methods, and procedures used to accomplish an organization's mission, goals, and objectives. Internal controls protect assets, detect errors, and prevent fraud. Systems of internal controls provide reasonable assurance that the following objectives are being achieved: 1) effectiveness and efficiency of operations; 2) reliability of financial reporting; and 3) compliance with applicable laws and regulations.

The Department of the Treasury developed the Joint Audit Management Enterprise System (JAMES) to track issues, findings, and recommendations reported in Government Accountability Office (GAO), Treasury Inspector General, and Treasury Inspector General for Tax Administration (TIGTA) audit reports. The JAMES is used to track the current progress of Planned Corrective Actions (PCA) for material weaknesses, significant deficiencies, and existing reportable conditions as well as remediation and action plans. Tracking issues, findings, recommendations, and the current progress of PCAs is also mandatory to comply with the intent of the GAO's *Standards for Internal Control in the Federal Government*,[2] the Federal Managers' Financial Integrity Act of 1982,[3] Office of Management and Budget Circulars, and Treasury Directives. The information contained in the JAMES is used by the Department of the Treasury to assess the effectiveness and progress of its bureaus in correcting their internal control deficiencies and implementing audit recommendations. The JAMES allows Department of the Treasury bureau users to run reports to assess the effectiveness of their programs.

On October 1, 2015, the Office of Audit Coordination took over responsibility for managing JAMES-related activities from the Office of Internal Controls.[4] The Office of Audit Coordination, in the Office of the Chief Financial Officer (CFO), supports the day-to-day internal control program for the Internal Revenue Service (IRS), including audit follow-up activities. Figure 1 provides the current organizational structure for the Office of the CFO.

---

[1] See Appendix VI for a glossary of terms.
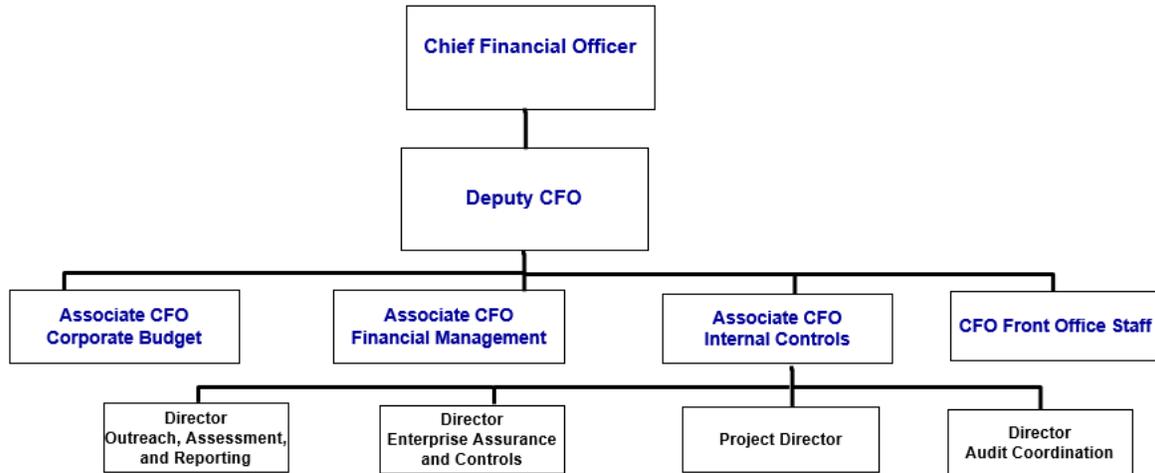[2] GAO-14-704G (Sept. 10, 2014).
[3] 31 U.S.C. §§ 1105, 1113, and 3512 (2013).
[4] We will use "Office of Audit Coordination" throughout the report for consistency.

Figure 1: Partial Organizational Chart for the Office of the CFO

Source: Office of the CFO (May 29, 2018).

IRS management is responsible for ensuring that the PCAs are implemented. In addition, IRS management is responsible for assigning individuals within the respective business units to serve as JAMES audit coordinators. The JAMES audit coordinators' responsibilities include uploading Form 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/ SD/TAS/REM Reports*,[5] and documentation supporting each PCA closure into the JAMES. All business units use Form 13872 to update the status of their PCAs in the JAMES, *e.g.*, adding the PCA implementation date or extending the due date. Further, JAMES audit coordinators are responsible for ensuring that supporting documentation is sufficient and maintained for five years. Figure 2 summarizes the JAMES PCA creation and closure process used by the IRS.

---

[5] MW = Material Weaknesses, SD = Significant Deficiencies, TAS = Taxpayer Advocate Service, and REM = Remediation Plans.

Figure 2: The JAMES PCA Creation and Closure Process

TIGTA Findings
- TIGTA conveys findings and recommendations to IRS management in a draft audit report.
- IRS management provides a formal response to TIGTA's draft audit report indicating disagreement or agreement with the recommendations and describing the PCAs, responsible officials, and implementation dates.

Audit Report
- TIGTA issues the final audit report with the IRS's formal management response and any Office of Audit comments addressing the IRS's response and the PCAs, if warranted.
- TIGTA enters the findings, recommendations, and PCAs into the JAMES.

JAMES
- The JAMES audit coordinators manage the corrective actions from planning to implementation, uploading supporting documentation to the JAMES.
- The responsible official reviews the supporting documentation and approves Form 13872 for PCA closure.
- The Office of Audit Coordination validates the status updates for reasonableness and records the PCA as closed.

Source: Internal Revenue Manual 1.4.30.

This review was performed at the Information Technology organization's Strategy and Planning, Applications Development, and Enterprise Operations offices at the New Carrollton Federal Building in Lanham, Maryland, during the period November 2017 through May 2018. 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.

Results of Review

To assess the IRS's PCA closure process, we selected for review a judgmental sample[6] of 20 PCAs from a total population of 203 PCAs pertaining to prior TIGTA recommendations related to IRS systems development and operations closed as implemented between October 2012 and September 2016.[7] We selected PCAs for our sample for what we considered to be higher risk issues identified in prior TIGTA audit reports. We excluded any cybersecurity-related PCAs because TIGTA is conducting a separate review of those PCAs.

Our review of the sampled PCAs found that approving officials and the Office of Audit Coordination approved each PCA closure. However, the PCA closure process, including ensuring that PCAs are fully implemented, needs to be improved.

The Planned Corrective Action Closure Process Needs Improvement

The "Specific action taken" section of some Forms 13872 did not include complete descriptions of the actions taken

According to the instructions for Form 13872, the "Specific action taken" section of the form should state the specific activities taken to implement the agreed-upon action(s). Based on our review, the "Specific action taken" section of Form 13872 did not completely describe how the IRS implemented the PCAs for two (12.5 percent) of 16 sampled PCAs.[8] For example, the forms for two PCAs did not provide any details on how the IRS implemented corrective actions for the Tier II backup hardware and the Tier II software upgrades. The forms simply stated that the upgrades were completed. In both examples, the information on the forms did not comply with PCA closure instructions to document the specific activities taken to implement the PCAs. Without a complete description of actions taken to implement the PCAs, it is unclear how or to what extent the IRS implemented them.

PCA closures were approved, but sufficient documentation was not uploaded to the JAMES

According to Internal Revenue Manual 1.4.30, it is the responsibility of JAMES audit coordinators and the Office of Audit Coordination to ensure that adequate documentation is

---

[6] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[7] Appendix V provides the results of our sample review.
[8] Our sample was comprised of 20 closed PCAs, which included four PCAs that were closed with management's response prior to April 1, 2017. Prior to April 1, 2017, the IRS did not require personnel to upload supporting documentation to the JAMES for PCAs closed at the time of management's response.

uploaded to the JAMES before PCAs are closed. We reviewed supporting documentation in the JAMES for the 16 sampled PCAs and found that the IRS did not upload sufficient supporting documentation to support proper PCA closure for six (37.5 percent) of them. The following provides further details of our analysis related to the insufficient supporting closure documentation in the JAMES.

- **PCA Sample Number 1:** The IRS provided evidence that Online 5081 records were resubmitted for only four of the 27 source system service accounts identified. We asked for evidence that the IRS had updated access authorization documentation for the remaining accounts; however, the IRS did not provide us any further documentation.

- **PCA Sample Number 7:** Although there was a PCA to ensure yearly training on the Error Resolution System (ERS) and the regular collection of some ERS analysis results, there was only one ERS yearly training schedule and no documented, collected, and reported ERS error analysis results uploaded to the JAMES. Subsequently, IRS management was able to provide us examples of the regular capture of ERS analysis results and yearly training schedules to verify proper closure of this corrective action.

- **PCA Sample Numbers 12 and 13:** For these two PCAs, the IRS uploaded into the JAMES only the requisition orders to support the Tier II backup hardware and Tier II software upgrades. Subsequently, IRS management was able to provide us additional supporting documentation in the form of purchase orders and invoices to verify proper closure of these corrective actions.

- **PCA Sample Number 15:** The IRS only uploaded to the JAMES a memorandum issued to the business unit commissioners reminding them of the need to comply with Internal Revenue Manual requirements and requesting assistance in adhering to the new processes and procedures for managing and governing the IRS SharePoint environment. We requested that the IRS provide additional documentation to show that it had enabled audit trails of key user activities on its SharePoint sites and reviewed these audit trails on a regular basis. Subsequently, IRS management provided us documentation which showed that they had implemented a quarterly review of the SharePoint audit logs and were able to identify and log key user activities.

- **PCA Sample Number 18:** As supporting closure documentation, IRS management uploaded a memorandum to the JAMES that they had issued to the business unit commissioners reminding them of the requirement for SharePoint site collection administrators to validate the presence of Personally Identifiable Information (PII) or Sensitive But Unclassified (SBU) data on their sites. We requested that the IRS provide additional evidence to validate that the site collection administrators had correctly self-certified sites as having PII or SBU data and had subsequently completed Privacy and Civil Liberties Impact Assessments. While the IRS provided us self-certifications that the site collection administrators had completed, the IRS was unable to provide any

further documentation to support that all IRS SharePoint sites with PII or SBU data requiring Privacy and Civil Liberties Impact Assessments were identified.

Based on the sampled PCAs we reviewed, we determined that JAMES audit coordinators and the Office of Audit Coordination did not always ensure that sufficient documentation was uploaded into the JAMES to support PCA closure. Without sufficient supporting documentation in the JAMES, there is limited evidence to support that the sampled PCAs were fully implemented.

PCAs closed with IRS management's response to the audit report

As of April 1, 2017, the Office of Audit Coordination implemented a policy that required supporting documentation to be captured for all PCAs, including those closed with the IRS management's response to the audit report. Although not in our initial sample of 20 judgmentally selected PCAs, the IRS requested that we look at compliance with this new policy. We identified one audit report[9] for testing that included a PCA that was closed with management's response. From our review, we determined that the IRS provided sufficient documentation to support the implementation and closure of this additional sampled PCA and complied with its new policy.

Management Action

In response to a prior TIGTA audit report,[10] the CFO implemented a quarterly quality control process to review a statistical sample of PCAs to ensure that sufficient supporting documentation was captured in the JAMES. We examined evidence that the Office of Audit Coordination had conducted a review of a random sample of PCAs for the period of October 2016 through December 2017. Although we did not test the thoroughness of these reviews, we believe that if these periodic reviews are conducted as planned, they will assist management with providing some assurance that the IRS is fully implementing its PCAs.

The PCA closure process does not require managers implementing corrective actions to approve their closure

The IRS instructions for completing Form 13872 do not require the manager responsible for implementing the PCA to review, approve, and sign the form to close the PCAs. If both the manager responsible for implementing the PCA and his or her executive would approve the closure of the PCA, this would help to establish accountability as required by the GAO's *Standards for Internal Control in the Federal Government*, which is for management to hold personnel accountable for performing their assigned internal control responsibilities. This would also provide an additional level of control to help ensure that PCAs are fully implemented as well as hold the persons directly involved in the PCAs' implementation responsible for ensuring

---

[9] TIGTA, Ref. No. 2017-20-057, *While Release 1.0 of the Web Applications System Was Successfully Deployed, Several Factors Contributed to Implementation Delays* (Sept. 2017).
[10] TIGTA, Ref. No. 2013-20-117, *Improved Controls Are Needed to Ensure That All Planned Corrective Actions for Security Weaknesses Are Fully Implemented to Protect Taxpayer Data* (Sept. 2013).

that sufficient supporting documentation was uploaded to the JAMES. Without the responsible managers approving the Form 13872, there is a greater risk that PCAs will not be fully implemented and supporting documentation in the JAMES will not be sufficient to support PCA closure.

Recommendations

The CFO should ensure that:

Recommendation 1*:* Complete descriptions of the specific actions taken to close PCAs are documented on Forms 13872.

> ***Management's Response:*** The IRS agreed with this recommendation. The Internal Controls organization is updating the Internal Revenue Manual for the Office of Audit Coordination. The Internal Controls organization will review and update, as necessary, existing policy to ensure that program owners are required to completely document actions taken to satisfy PCA closure requirements.

Recommendation 2: Sufficient supporting documentation is uploaded to the JAMES to support PCA closure.

> ***Management's Response:*** The IRS agreed with this recommendation. The Office of Audit Coordination will continue to conduct reviews throughout the year of a sample of closed PCAs to ensure that the IRS meets documentation requirements. As the IRS updates the Audit Coordination Internal Revenue Manual and guidance, it will evaluate the existing review criteria to determine if the criteria needs to be improved.

Recommendation 3: The Internal Revenue Manual and instructions for Form 13872 are updated so that both the manager responsible for implementing the PCA and the executive responsible for the PCA are required to approve Form 13872 supporting the PCA's closure.

> ***Management's Response:*** The IRS agreed with this recommendation. The Internal Controls organization is updating the Internal Revenue Manual for the Office of Audit Coordination. Form 13872 will be modified concurrently with the Internal Revenue Manual update.

## *Closed Planned Corrective Actions Were Not Fully Implemented*

According to Internal Revenue Manual 1.4.30, IRS management should ensure that recommendations are implemented. Through the JAMES, we analyzed available documents and, when necessary, requested additional supporting documentation from the JAMES audit coordinators and responsible Information Technology organization functions to validate if the IRS had fully implemented the 20 sampled closed PCAs.

To validate that our sampled PCAs had been fully implemented by the IRS, we reviewed whether agency officials had sufficient documentation, as defined in the GAO's *Government Auditing Standards*,[11] to persuade a knowledgeable person that the conclusions and findings are reasonable. Figure 3 presents our overall assessment regarding the 20 closed PCAs selected in our sample.

**Figure 3: TIGTA's Assessment of
Sampled Closed PCA Implementation**

PCAs Not Implemented 1 (5%)

PCAs Partially Implemented 3 (15%)

PCAs Implemented 16 (80%)
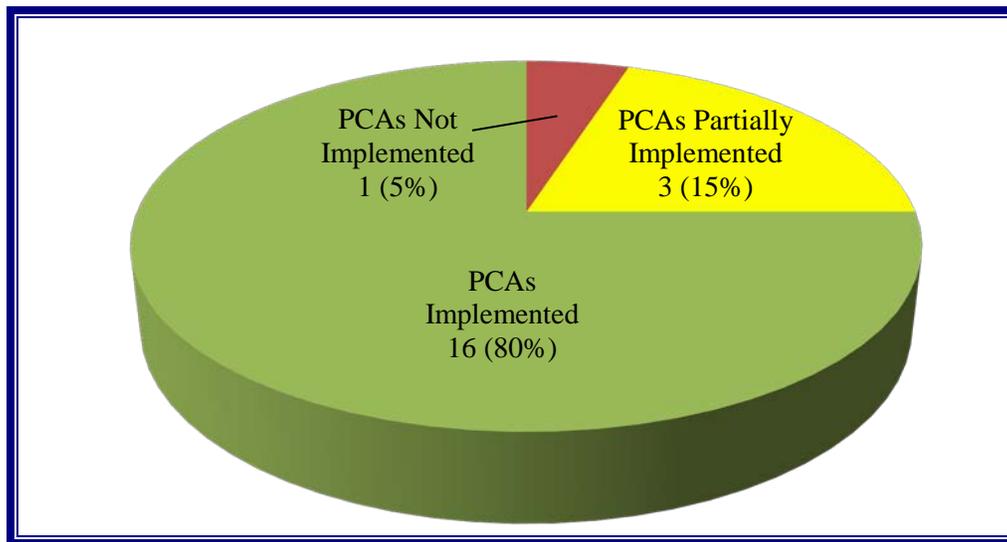
Source: TIGTA analysis of 20 sampled PCAs closed during Fiscal Years 2013 through 2016.

We found that the IRS did not fully implement four (20 percent) of the 20 sampled PCAs that it had closed as implemented on the JAMES. Of these four PCAs, we found that three PCAs were partially implemented and one PCA was not implemented at all. The following provides further details of our analysis related to the closed PCAs that were not fully implemented.

- **PCA Sample Number 1:** According to this closed PCA, the IRS's Integrated Production Model project team was to resubmit Online 5081 records for each source system service account to document the access authorization. The IRS provided evidence that Online 5081 records were resubmitted for only four of the 27 source system service accounts identified in a prior TIGTA audit report.[12] Therefore, based on the insufficient documentation and discussion with the responsible Information Technology organization function, we confirmed that the PCA was not fully implemented and was closed prematurely.

---

[11] GAO-12-331G (Dec. 1, 2011).

[12] TIGTA, Ref. No. 2016-20-058, *The Integrated Production Model Increases Data Access Efficiency; However, Access Controls and Data Validation Could Be Improved* (July 2016).

- **PCA Sample Number 14:** According to this closed PCA, the IRS was to ensure that personnel are granted appropriate authorization to perform backup and restore functions. We requested supporting documentation regarding how the IRS implemented this recommendation. However, the IRS did not provide any supporting documentation that it had reviewed the privilege groups of administrators with the capability to perform backup and restore duties.

- **PCA Sample Number 17:** According to this closed PCA, the IRS identified, deployed, and executed an automated tool to identify SharePoint sites containing PII or SBU data. The IRS provided documentation that an automated tool was installed in the production environment as of October 2016. However, based on discussions with responsible officials and review of supporting documentation, the tool did not work consistently to identify PII or SBU data on the IRS SharePoint production sites. The tool was problematic and only partially identified SharePoint sites containing PII or SBU data. Subsequently, the IRS purchased another automated tool that, according to IRS management, will not be placed into production until September 2018. Because the old tool was unable to completely identify PII or SBU data on the IRS SharePoint sites as well as the new tool still being tested, this PCA was not fully implemented prior to its closure on the JAMES.

- **PCA Sample Number 18:** According to this closed PCA, the IRS should ensure that SharePoint site collections containing PII or SBU data have approved Privacy and Civil Liberties Impact Assessments. IRS management provided a memorandum in the JAMES that they had issued to the business unit commissioners reminding them of the requirement for site collection administrators to validate the presence of PII or SBU data on their sites.

  Site collection administrators self-certify if their SharePoint sites contain PII or SBU data. If a site collection administrator certifies that his or her SharePoint site contains PII or SBU data, he or she is required to complete a Privacy and Civil Liberties Impact Assessment and send it to the Office of Privacy, Governmental Liaison, and Disclosure. Because independent verifications of the self-certifications are not performed and the previous automated tool that the IRS selected did not reliably identify the PII or SBU data on its SharePoint sites, there are limited manual controls in effect to ensure that site collection administrators correctly self-certify PII or SBU sites and complete Privacy and Civil Liberties Impact Assessments. By not fully implementing an automated tool, there is no assurance that the PCA to ensure that SharePoint site collections containing PII or SBU data have approved Privacy and Civil Liberties Impact Assessments was fully implemented.

For these four sampled PCAs, the IRS did not provide sufficient evidence to support a conclusion that these PCAs had fully been implemented. As a result, the IRS continues to be vulnerable to negative impacts of not addressing previously reported and agreed-to weaknesses

in its controls. In addition, by not fully implementing these PCAs, realization of program benefits related to IRS management of taxpayer data and organizational improvements could be negatively affected.

Recommendation

Recommendation 4*:* The Chief Information Officer (CIO) should ensure that the prematurely closed PCAs are reopened and monitored until fully implemented.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will reopen and monitor, until fully implemented, the three PCAs that were prematurely closed.

> ***Office of Audit Comment:*** There were four PCAs identified during this review that were prematurely closed off of the JAMES. The PCA related to the Integrated Production Model is no longer current due to system changes. The IRS will add information of actions taken to the JAMES to support its closure.

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether closed corrective actions reported by the IRS's Information Technology organization from prior TIGTA audits have been adequately documented, appropriately approved, and fully implemented. To accomplish our objective, we:

I. Identified the controls inherent in the IRS's PCA closure process.

  A. Interviewed Office of Audit Coordination personnel to conduct a walkthrough and document their responsibilities over the JAMES process.

  B. Obtained and reviewed policies, procedures, and guidelines related to identifying, tracking, and closing corrective actions in the JAMES.

II. Determined whether closed corrective actions were adequately documented by IRS personnel.

  A. Requested from TIGTA's Management Planning and Workforce Development Division the Form 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports*,[1] and any supporting documents for a judgmental sample[2] of 20 PCAs closed during Fiscal Years 2013 through 2016 to determine whether the information uploaded into the JAMES supported closure of each selected PCA. The sampled PCAs were from a total population of 203 closed PCAs involving IRS systems development and operations recommendations in prior TIGTA audit reports that we determined were higher risk recommendations. We excluded any cybersecurity-related PCAs because TIGTA is conducting a separate review of those PCAs.

  1. Reviewed each Form 13872 to determine whether the corrective action was sufficiently documented.

  2. Reviewed any supporting documents to determine whether they support full and timely closure of each selected corrective action. If documents in the JAMES were not sufficient, we contacted the appropriate JAMES audit coordinator(s) or responsible business unit(s) to obtain and review any additional supporting documentation kept outside of the JAMES that supported the closure of each selected corrective action.

---

[1] MW = Material Weaknesses, SD = Significant Deficiencies, TAS = Taxpayer Advocate Service, and REM = Remediation Plans.

[2] A judgmental sample is a nonprobability sample, the results of which cannot be projected to the population.

B. If the Form 13872 and supporting documentation were not sufficient to explain what and how corrective actions were implemented, we discussed our conclusions with the appropriate IRS personnel to obtain agreement to the facts.

III. Determined whether closed corrective actions were appropriately approved by IRS management.

A. Reviewed Form 13872 for each selected closed corrective action to ensure that it contained an executive approval by the responsible official.

B. Obtained and reviewed any documentation of the Office of Audit Coordination review for each closed corrective action.

IV. Determined whether closed corrective actions were fully implemented as of July 31, 2017.

A. Assessed whether the sampled corrective actions were fully implemented.

B. If audit tests indicated that the corrective actions were not fully implemented, discussed our conclusions with the appropriate IRS personnel to obtain agreement to the facts.

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: CIO and CFO policies, procedures, and processes for managing and ensuring the proper closure of PCAs. We evaluated these controls by interviewing CIO and CFO personnel, identifying guidance for managing and ensuring PCA closure and implementation, reviewing documents supporting the closure of the PCAs, and independently assessing the PCA closure process.

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Bryce Kisler, Director
Carol Taylor, Audit Manager
Denis Danilin, Lead Information Technology Specialist
Mark Carder, Senior Auditor

Report Distribution List

Deputy Commissioner for Operations Support
Chief Financial Officer
Chief Information Officer
Deputy Chief Financial Officer
Deputy Chief Information Officer for Operations
Associate Chief Financial Officer for Internal Controls
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise-Program Management Office
Associate Chief Information Officer, Strategy and Planning
Director, Office of Audit Coordination

Improved Controls Are Needed to Ensure That Corrective Actions for Reported Information Technology Weaknesses Are Documented and Fully Implemented Prior to Closure

Appendix IV

Outcome Measures

This appendix presents information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; two of 16 Forms 13872, *Planned Corrective Action (PCA) Status Update for TIGTA/GAO/MW/SD/TAS/REM Reports*,[1] did not include complete descriptions of the efforts taken by the IRS to close the PCAs (see page 4).

Methodology Used to Measure the Reported Benefit:

We reviewed a judgmental[2] sample of 20 PCAs and any related supporting documentation. For sample items that required supporting documentation,[3] our analysis identified that two of the 16 Forms 13872 did not include complete descriptions of the IRS's efforts to close the PCAs.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; six closed PCAs had insufficient documentation in the JAMES to support their closure (see page 4).

Methodology Used to Measure the Reported Benefit:

Using the same judgmental sample of 20 PCAs mentioned previously, we found that six sampled PCAs had insufficient documentation in the JAMES to support their closure.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; two closed PCAs were not fully implemented and were prematurely closed, which resulted in incorrect information being recorded in the JAMES (see page 7).

---

[1] MW = Material Weaknesses, SD = Significant Deficiencies, TAS = Taxpayer Advocate Service, and REM = Remediation Plans.

[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

[3] Our sample was comprised of 20 closed PCAs, which included four PCAs that were closed with management's response prior to April 1, 2017. Prior to April 1, 2017, the IRS did not require personnel to upload supporting documentation to the JAMES for PCAs closed at the time of management's response.

Methodology Used to Measure the Reported Benefit:

Using the judgmental sample of 20 PCAs mentioned previously, we found that four sampled PCAs were not fully implemented and were prematurely closed, which resulted in incorrect information being recorded in the JAMES. However, two of these PCAs also had insufficient documentation to support their closure as well as not being fully implemented and thus prematurely closed off the JAMES. These two PCAs were included in the count total of the prior outcome measure.

Assessment of the Information Technology Organization's Planned Corrective Actions

PCA Sample Number	Recommendations	PCAs	TIGTA's Assessment of PCA Status
TIGTA, Ref. No. 2016-20-058, *The Integrated Production Model Increases Data Access Efficiency; However, Access Controls and Data Validation Could Be Improved* (July 2016).			
1	The Chief Technology Officer[1] (CTO) should establish updated access authorization documentation for the Integrated Production Model[2] in each of the source systems.	The Integrated Production Model will resubmit Online 5081 records for each source system service account to document the access authorization.	**Partially Implemented** The IRS could not provide supporting documentation that it had resubmitted Online 5081 records for all 27 source system service accounts.
TIGTA, Ref. No. 2013-20-013, *The Data Center Consolidation Initiative Has Made Significant Progress, but Program Management Should Be Improved to Ensure That Goals Are Achieved* (June 2013).			
2	The CTO should update the annual inventory submitted to the Department of the Treasury to include all data centers regardless of size.	The IRS will update the annual inventory submitted to the Department of the Treasury to include all data centers.	**Implemented**
TIGTA, Ref. No. 2013-20-089, *Weaknesses in Asset Management Controls Leave Information Technology Assets Vulnerable to Loss* (Sept. 2013).			
3	The CTO should ensure that Knowledge Incident/Problem Service Asset Management – Asset Manager records are updated to correct the deficiencies identified in our review and provided to management.	The IRS will perform data review and analysis to correct deficiencies identified by TIGTA and will update the Knowledge Incident/Problem Service Asset Management – Asset Manager accordingly with current and complete information.	**Implemented**
4	The CTO should create additional anomaly reports for the minimum required Knowledge Incident/Problem Service Asset Management – Asset Manager data fields to facilitate ensuring that only valid entries are provided.	The IRS will engage asset owners and stakeholders to solicit feedback and requirements for new asset data anomaly reports to facilitate anomaly resolution and verification activities. Any necessary new reports will be created.	**Implemented**

---

[1] As of July 2016, the IRS changed the title of this executive leadership position to the Chief Information Officer.
[2] See Appendix VI for a glossary of terms.

PCA Sample Number	Recommendations	PCAs	TIGTA's Assessment of PCA Status
5	The CTO should include dollar threshold criteria in the Certification Plan for certifying information technology assets with a high-dollar value that affect financial statement reporting.	The IRS will update the Fiscal Year 2014 and all future inventory Certification Plans to require that assets with an acquisition value of $50,000 or greater be verified and certified.	**Implemented**
TIGTA, Ref. No. 2015-23-062, *Affordable Care Act Information Sharing and Reporting Project* (Aug. 2015).			
6	The CTO should ensure that the Information Sharing and Reporting Project Risk Management Plan is updated to clearly reflect its high priority and high-impact risk and issue elevation process.	The Information Sharing and Reporting Project will implement changes to its high priority and high-impact risk and issue elevation process and will make needed updates to the Risk Management Plan for better monitoring and escalation of risks and issues as part of the Enterprise Life Cycle defined process for documentation updates.	**Implemented**
TIGTA, Ref. No. 2014-20-085, *Increased Support Is Needed to Ensure the Effectiveness of the Final Integration Test* (Sept. 2014).			
7	To ensure that the Final Integration Test results are used to improve the program, the CTO should establish a process to determine the reason Final Integration Test tax returns go to the ERS and use those results to identify training opportunities or operational improvements.	The IRS agreed that further ERS training is required to reduce the error analysis results during the annual Enterprise Systems Testing. It is taking steps to implement this recommendation and has initiated ERS training sessions to address common fallout errors. Enterprise Systems Testing will continue to leverage the current test-tracking tool, Rational Quality Manager, to document, track, and report ERS data results. Further, modifications to existing test-tracking tools have been initiated to document, collect, and report ERS error analysis results for the 2015 Filing Season effort. The collection and analysis of these data will provide insight to ERS processing performance goals.	**Implemented**

PCA Sample Number	Recommendations	PCAs	TIGTA's Assessment of PCA Status
TIGTA, Ref. No. 2015-23-081, *Affordable Care Act Verification Service: Security and Testing Risks* (Sept. 2015).			
8	The CTO should ensure that testing organizations use only the information from the designated tools for documenting requirements, test results, and defects to prepare the End-of-Test Completion Report.	The testing organization will document this issue in Lessons Learned and will reiterate the processes/procedures for creating the End-of-Test Completion Reports with the analysts.	**Implemented**
9	The CTO should ensure that developers are notified in advance when changes to the development, test, and production environments are made to ensure that the programs being developed are compatible with the updated environments.	The IRS has instituted an Environment Work Group, which meets biweekly and communicates a variety of environment-related information, including when changes or updates are made.	**Implemented**
TIGTA, Ref. No. 2014-20-016, *Planning Is Underway for the Enterprise-Wide Transition to Internet Protocol Version 6, but Further Actions Are Needed* (Feb. 2014).			
10	The CTO should develop and distribute an Information Resources Management Strategic Plan as originally described in the 2014 IPv6 [Internet Protocol Version 6] Transition Plan and involve Agency-Wide Shared Services' Information Technology Procurement function with the plan's development. This planning effort should also establish a process to communicate and incorporate future changes or enhancements to the Information Resources Management Strategic Plan.	The IRS will revise the Information Technology Integrated Release Plan, referred to as the Information Resources Management Strategic Plan in the 2014 IPv6 Transition Plan, to incorporate IPv6. Information Technology Strategy and Planning and Agency-Wide Shared Services Office of Procurement will annually conduct a review of the plan to update the document with future IPv6 changes.	**Implemented**
11	The CTO should ensure that the IPv6 project team coordinates with the Enterprise Life Cycle office and takes a more proactive role of adhering to the process and meeting project milestone deadlines to ensure the timely completion of key deliverables, artifacts, and processes for the critical 2014 enterprise-wide transition to IPv6.	Due to budget and schedule constraints, a risk-based decision was made to complete Enterprise Life Cycle milestone 1 and 2 artifacts for the Fiscal Year 2012 mandate. The Enterprise Life Cycle Project Office approved an IPv6 Tailoring Plan in July 2013 that combined the Fiscal Years 2012 and 2014 mandates. The IPv6 Program Management Office will complete future deliverables in accordance with the approved Tailoring Plan.	**Implemented**

PCA Sample Number	Recommendations	PCAs	TIGTA's Assessment of PCA Status
TIGTA, Ref. No. 2016-20-019, *Management Oversight of the Tier II Environment Backup and Restoration Process Needs Improvement* (Feb. 2016).			
12	The CTO should upgrade the software for the Tier II backup environment to meet Federal requirements and operational needs as resources are identified.	The IRS will upgrade the Tier II backup software to the most current version, contingent upon funding, aligning with IRS processes and procedures to assess, prioritize, and implement currency-related upgrades.	**Implemented**
13	The CTO should upgrade the aged Tier II backup environment hardware infrastructure as resources are identified.	The IRS will upgrade the aged Tier II backup environment hardware infrastructure, contingent upon funding, aligning with IRS processes and procedures to assess, prioritize, and implement currency-related upgrades.	**Implemented**
14	The CTO should identify and review all privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel are granted appropriate authorization.	The IRS reviewed the privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel had appropriate authorization.	**Not implemented** The IRS could not provide supporting documentation that the IRS reviewed the privilege groups of administrators with the capability to perform backup and restore duties to ensure that personnel had appropriate authorization.
TIGTA, Ref. No. 2016-20-075, *Information Technology: SharePoint Controls Need Improvement to Mitigate Risks and to Ensure That Possible Duplicate Costs Are Avoided* (Sept. 2016).			
15	The CIO should coordinate with the respective business unit commissioners to ensure that the SharePoint site collection owners and administrators enable audit trails of key user activities on their sites and that they review audit trails on a regular basis.	The IRS partially agreed with the recommendation. The IRS will ensure that audit trails are enabled to capture all key user activities on all SharePoint sites. The IRS will also issue a memorandum to all business unit commissioners to remind them of the Internal Revenue Manual requirement that site collection owners and administrators review audit trails on a regular basis.	**Implemented**
16	The CIO should ensure that the draft SharePoint Information Technology Contingency Plan, including a Business Impact Analysis, is finalized and approved by management.	The draft SharePoint Information Technology Contingency Plan is being updated to reflect the current environment and will be submitted for review to finalize the document.	**Implemented**

PCA Sample Number	Recommendations	PCAs	TIGTA's Assessment of PCA Status
17	The CIO should ensure that an automated tool is identified, deployed, and routinely executed to identify SharePoint sites containing PII and SBU data.	The IRS ensured that an automated tool was identified, deployed, and executed to identify SharePoint sites containing PII or SBU data.	**Partially Implemented** This PCA was not fully implemented because the old automated tool was unable to fully identify PII or SBU data on the IRS SharePoint sites and the new tool has not been fully implemented.
18	The CIO should ensure that SharePoint site collections containing PII or SBU data have approved Privacy and Civil Liberties Impact Assessments.	The IRS will ensure that SharePoint site collections containing PII or SBU data have approved Privacy and Civil Liberties Impact Assessments.	**Partially Implemented** Site collection administrators self-certify if their SharePoint sites contain PII or SBU data. Because independent verifications of the self-certifications are not performed and the previous automated tool that the IRS selected did not reliably identify the PII or SBU data on its SharePoint sites, there are limited manual controls in effect to ensure that site collection administrators correctly self-certify PII or SBU sites and complete Privacy and Civil Liberties Impact Assessments. By not fully implementing an automated tool, there is no assurance that the PCA to ensure that SharePoint site collections containing PII or SBU data have approved Privacy and Civil Liberties Impact Assessments was fully implemented.
19	The CIO should coordinate with the respective business unit commissioners to ensure that the SharePoint governance structure is enhanced to provide enterprise adherence to SharePoint security and content management policies.	The IRS will ensure coordination with the respective business [unit] commissioners' SharePoint Governance Board representatives so the SharePoint governance structure, where needed, is enhanced to provide enterprise adherence to SharePoint security and content management policies.	**Implemented**

PCA Sample Number	Recommendations	PCAs	TIGTA's Assessment of PCA Status
TIGTA, Ref. No. 2016-20-080, *Review of the Enterprise E-Mail System Acquisition* (Sept. 2016).			
20	The CIO should seek a review by IRS Chief Counsel to determine if the purchase of Microsoft Office 365 ProPlus and Exchange Online violated the *bona fide* needs rule and take any actions required by law.	The CIO has requested that Chief Counsel determine if the purchase of Microsoft Office 365 ProPlus and Exchange Online violated the *bona fide* needs rule. Upon completion of the Chief Counsel's response, the IRS will take any action required.	**Implemented**

*Improved Controls Are Needed to Ensure That Corrective
Actions for Reported Information Technology Weaknesses
Are Documented and Fully Implemented Prior to Closure*

Appendix VI

Glossary of Terms

Term	Definition
Anomaly Report	Produced annually to identify inconsistencies or potential inaccuracies in the Knowledge Incident/Problem Service Asset Management – Asset Manager database.
Application	An information technology component of a system that uses information technology resources to store, process, retrieve, or transmit data or information using information technology hardware and software.
Audit Trail	A record of system activity, both by system and application processes and by user activity on systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Business Unit	A title for major IRS organizations such as Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and the Information Technology organization.
Database	A computer system with a means of storing information in such a way that information can be retrieved.
End-of-Test Completion Report	A required report that summarizes the completed system project-level and system-release–level test effort for the release.
Enterprise Life Cycle	The approach used by the IRS to manage and effect business change. The Enterprise Life Cycle provides the direction, processes, tools, and assets for accomplishing business change in a repeatable and reliable manner.

Term	Definition
Error Resolution System	An IRS application that provides for the correction of errors associated with input submissions. The error inventory is managed on a database, and corrected documents are validated by the Generalized Mainline Framework system.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Final Integration Test	A system test consisting of integrated end-to-end testing of mainline tax processing systems to verify that new releases of interrelated systems and hardware platforms can collectively support IRS business functions.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
Generalized Mainline Framework	The system used to process and control all documents through the submission processing campus pipeline.
Governance	A set of processes, guidelines, and policies that guide and affect the direction of an organization's behavior or assets.
Integrated Production Model	A consolidated source of core taxpayer data, *e.g.*, tax account, tax return, and third-party data, and business application data to be used by a wide range of business applications to support case identification, selection, prioritization, and delivery.
Internal Revenue Manual	The IRS's primary source of instructions to its employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Internet Protocol Version 6	The next generation Internet Protocol that allows a 128-bit Internet Protocol address field in the form of eight 16-bit integers to be represented as four hexadecimal digits separated by colons.
Knowledge Incident/Problem Service Asset Management System	An IRS application that maintains the complete inventory of information technology and non–information technology assets, computer hardware, and software. It is also the reporting tool for problem management with all IRS-developed applications.

Term	Definition
Online 5081	The IRS's web-based Online 5081 system that is used to request access, modify existing accounts, reset passwords, and request deletion of accounts when access is no longer needed to specific systems.
Personally Identifiable Information	Any information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, and mother's maiden name.
Privacy and Civil Liberties Impact Assessment	An analysis of how information in an identifiable form is collected, stored, protected, shared, and managed. The process also provides a means to assure compliance with all applicable laws and regulations governing taxpayer and employee privacy.
Release	A specific edition of software.
Sensitive but Unclassified	A designation of information in the Federal Government that, though unclassified, often requires strict controls over its distribution.
SharePoint	A web-based repository that the IRS uses to store and control organizational products and documentation.
SharePoint Site	A site that allows the IRS to organize and store content in SharePoint; the content can be lists, libraries (document, picture, report, and form), web pages, or sites. Further, a site can have subsites in its hierarchy.
System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.
Tier II Environment	The computing environment that consists of non-mainframe servers. These servers run various operating systems, including versions of Microsoft Server, Linux, and UNIX. The servers may also operate as database, web, e-mail, and file servers, as well as provide a host of other important functions supporting the IRS network infrastructure.

**Improved Controls Are Needed to Ensure That Corrective
Actions for Reported Information Technology Weaknesses
Are Documented and Fully Implemented Prior to Closure**

Appendix VII

Management's Response to the Draft Report

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

AUG 2 7 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
                       Chief Information Officer

SUBJECT: Draft Audit Report –Improved Controls Are Needed to Ensure
                       Corrective Actions for Reported Information Technology
                       Weaknesses Are Documented and Fully Implemented Prior to
                       Closure (Audit # 201820013)

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

Internal controls are comprised of the plans, methods, and procedures used to
accomplish an organization's mission, goals, and objectives. The Chief Financial Officer
in conjunction with the Chief Information Officer has made substantial progress toward
ensuring complete descriptions of the specific actions taken to close Planned Corrective
Actions (PCAs) are documented in the Joint Audit Management Enterprise System
(JAMES). We will continue to closely monitor the program to ensure it stays on the right
track.

We are encouraged by your acknowledgement of the process improvements made by
the CFO since your last review. The recent consolidation of the Audit Coordination
office into the CFO's Internal Controls organization helps us to align efforts to improve
the identification, remediation and documentation of control issues as well as better
communicate the importance of internal controls throughout the IRS. Internal Controls is
already engaged in the development of updated PCA-related guidance, and will
incorporate your recommendations into that process moving forward.

Regarding the four PCAs you identified as partially or not implemented, we will add
additional evidence to the JAMES to support the closure of the PCA related to IRS's
Integrated Production Model, and re-open the other PCAs and monitor them until fully
implemented.

2

We are committed to continuously improving our information technology strategies, systems, and processes. The continued support, assistance, and guidance your team provides is very valuable to us in this regard. Our corrective action plan for the recommendations is attached. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Carmelita White at (240) 613-2191.

Attachment

Attachment

Draft Audit Report-IRS Responses to Recommendations:
*Improved Controls Are Needed to Ensure Corrective Actions for Reported Information
Technology Weaknesses Are Documented and Fully Implemented Prior to Closure*

RECOMMENDATION #1: Complete descriptions of the specific actions taken to close
PCAs are documented on Forms 13872.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. The Internal
Controls organization is updating the IRM for the Audit Coordination office. Internal
Controls will review existing policy and update it as necessary to ensure it is sufficiently
robust in requiring program owners to completely document actions taken to satisfy
closure requirements for PCAs.

IMPLEMENTATION DATE: May 15, 2019

RESPONSIBLE OFFICIAL: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: N/A – once the draft IRM entry is
complete, the Associate Chief Financial Officer for Internal Controls will submit it for
approval through the IRS IRM clearance process. The target publication date for the
new IRM is on or before the implementation date for this corrective action.

RECOMMENDATION #2: The Chief Financial Officer should ensure that sufficient
supporting documentation is uploaded to the JAMES to support PCA closure.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. The Audit
Coordination office will continue to conduct reviews of closed PCAs using an
appropriate sampling methodology throughout the year to ensure that the IRS meets
documentation requirements. As we update the Audit Coordination IRM and guidance,
we will evaluate the existing review criteria to determine if we need to improve them.

IMPLEMENTATION DATE: May 15, 2019

RESPONSIBLE OFFICIAL: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: N/A – once the draft IRM entry is
complete, the Associate Chief Financial Officer for Internal Controls will submit it for
approval through the IRS IRM clearance process. The target publication date for the
new IRM is on or before the implementation date for this corrective action.

Attachment

Draft Audit Report-IRS Responses to Recommendations:
Improved Controls Are Needed to Ensure Corrective Actions for Reported Information Technology Weaknesses Are Documented and Fully Implemented Prior to Closure

RECOMMENDATION #3: The Internal Revenue Manual and instructions for Form 13872 are updated so that both the manager responsible for implementing the PCA and the executive responsible for the PCA are required to approve Form 13872 supporting the PCA's closure.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. The Internal Controls organization is updating the IRM for the Audit Coordination office. Form 13872 will be modified concurrently with the IRM update.

IMPLEMENTATION DATE: May 15, 2019

RESPONSIBLE OFFICIAL: Associate Chief Financial Officer for Internal Controls

CORRECTIVE ACTION MONITORING PLAN: N/A – once the draft IRM entry is complete, the Associate Chief Financial Officer for Internal Controls will submit it for approval through the IRS IRM clearance process. Audit Coordination will coordinate with the IRS Media & Publications division to update Form 13872. The target publication date for both documents is on or before the implementation date for this corrective action.

RECOMMENDATION #4: The Chief Information Officer (CIO) should ensure that the prematurely closed PCAs are reopened and monitored until fully implemented.

CORRECTIVE ACTION #4: The IRS agrees with this recommendation. The IRS will re-open and monitor until fully implemented, the three PCAs that were prematurely closed (PCA sample ref. 14, 17 & 18).

IMPLEMENTATION DATE March 15, 2019

RESPONSIBLE OFFICIAL: Associate Chief Information Officer for Strategy and Planning

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