TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement

August 14, 2019

Reference Number: 2019-20-052

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

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

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

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

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

Information you provide is confidential and you may remain anonymous.

HIGHLIGHTS

INFORMATION TECHNOLOGY RISKS ARE IDENTIFIED, ASSESSED, AND REPORTED, BUT MITIGATION DOCUMENTATION AND OVERSIGHT NEED IMPROVEMENT

Highlights

Final Report issued on August 14, 2019

Highlights of Reference Number: 2019-20-052 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The Office of Management and Budget requires Federal agencies to implement a formal Enterprise Risk Management capability. Effective risk management can help the IRS, including its Information Technology organization, more securely and effectively administer the Federal tax system by identifying and mitigating emerging risks before they affect performance.

WHY TIGTA DID THE AUDIT

This audit was initiated to assess the effectiveness of the Information Technology organization's risk management process.

WHAT TIGTA FOUND

TIGTA's review focused on the identification, assessment, response, and reporting phases of the Information Technology organization's risk management process. The Information Technology organization's functions and programs are identifying, assessing, and reporting risks, but information on risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, is not being captured in sufficient detail to be useful.

The lack of detail is attributed, in part, to some functions using a risk management tool that does not capture essential information. For example, four functions use the Item Tracking Reporting and Control (ITRAC) system to track risks, while two functions use ProSight. There are two important fields captured in the ITRAC system that are not captured in ProSight: closure rationale and risk mitigation activity.

In addition, 18 function and 15 program risk records and related supporting information did not include complete descriptions or detailed documentation of the risk mitigation efforts. For example, the mitigation plan for a Foreign Account Tax Compliance Act risk stated, "Prepare Solaris contract extension, create environment, create barrier, remove tiger team," and the closure rationale provided was "Environments delivered" without providing any further details. Mitigation activities also were not detailed for this risk and there were no closure documents available.

Further, 19 of 20 accepted unmitigated risks were not reassessed quarterly as required by established guidance. For 16 of the risks, the reassessment dates were either scheduled or occurred at least one year or more after management officials accepted the risk.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer require: 1) all Information Technology organization functions (except the Cybersecurity function) to record risks in the ITRAC system; 2) detailed descriptions of the risk mitigation plans, mitigation activities, and closure rationale be captured and closure documentation be uploaded into the ITRAC system; 3) periodic review of the risk descriptions and documentation uploaded into the ITRAC system to ensure that the information is appropriate, current, complete, and accurate; and 4) a periodic reassessment of all accepted unmitigated risks to ensure that acceptance remains management's preferred response.

The IRS agreed with all of our recommendations. The IRS plans to require all Information Technology organization functions, except the Cybersecurity function, to use the ITRAC system; reinforce directions for capturing risks, mitigation plan descriptions, mitigation activities, and closure rationale and documentation; develop policy for periodic reviews of risk information in the ITRAC system; and modify processes to ensure that accepted unmitigated risks are reviewed at the appropriate time frames to confirm that risk acceptance remains the acceptable response or whether further action is needed.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 14, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement (Audit # 201820029)

This report presents the results of our review to assess the effectiveness of the Information Technology organization's risk management process. This review is included in our Fiscal Year 2019 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 VI.

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

Table of Contents

Appendices

Abbreviations

ACIO	Associate Chief Information Officer
ERM	Enterprise Risk Management
IRS	Internal Revenue Service
IT	Information Technology
ITRAC	Item Tracking Reporting and Control
OCRO	Office of the Chief Risk Officer
RAFT	Risk Acceptance Form and Tool
RBD	Risk-Based Decision

Background

The Internal Revenue Service (IRS) is a large and complex organization that faces significant ongoing internal and external risks in accomplishing its mission. These risks include having to manage a growing workload with substantially fewer employees, as well as implementing recent extensive tax law changes; the growing impact of international tax law issues; increasing sophistication of efforts to evade tax compliance; and cybersecurity threats to IRS-maintained taxpayer data.

The Office of Management and Budget requires Federal agencies to implement a formal Enterprise Risk Management (ERM) capability.[1] Specifically, Office of Management and Budget Circular No. A-123[2] defines management's responsibilities for the ERM and emphasizes the need to integrate risk management into existing business activities of an agency.

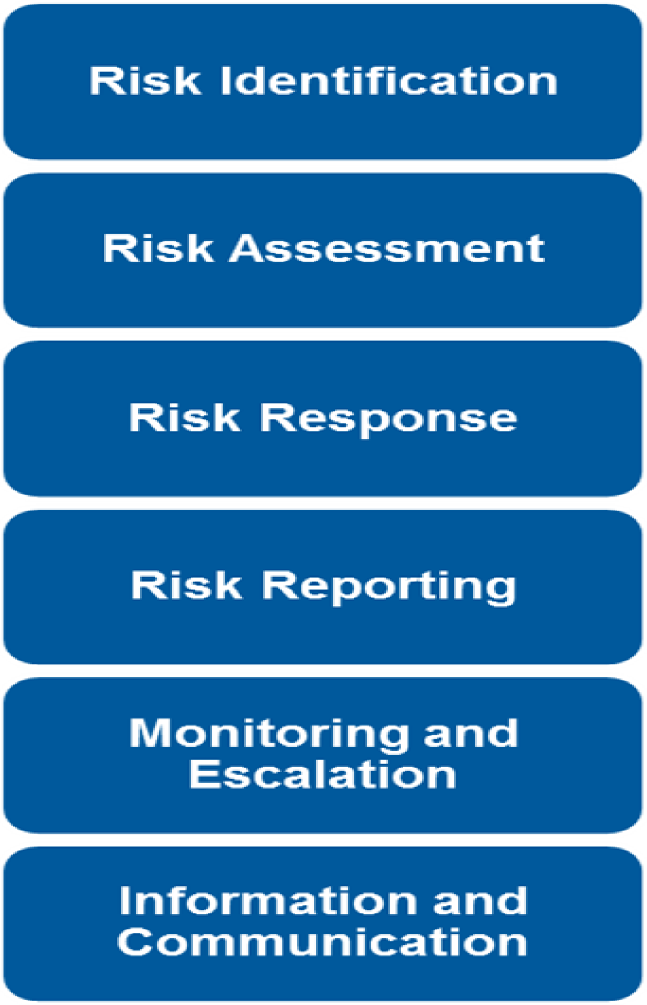
The IRS has appointed a Chief Risk Officer and established a risk management structure. The Chief Risk Officer oversees the ERM program to identify and assess risks, which provides an enterprise-wide approach to risk management and helps the IRS incorporate risk management principles into its strategies, providing senior management the information necessary to make sound decisions. The IRS has defined roles and responsibilities for the Chief Risk Officer, senior risk advisors, and ERM liaisons. The IRS also established an Executive Risk Committee, comprised of senior management, to facilitate collaboration on enterprise risk decisions and a Risk Working Group, which includes representatives from the various IRS business units and functional offices.

On an annual basis, the Office of the Chief Risk Officer (OCRO) facilitates an enterprise-wide risk assessment. The OCRO guidance specifies that business unit leadership should manage and monitor its risks on an ongoing basis. Accordingly, business units, including the Information Technology (IT) organization, provide a Business Unit Risk Register to the OCRO annually. The Business Unit Risk Register is a mechanism to document and monitor identified risks. The OCRO aggregates the results and provides initial reports to the Risk Working Group. The Risk Working Group analyzes the results from an enterprise perspective and works with the OCRO to develop a proposed enterprise risk list. Figure 1 lists the six phases of the IRS's risk management process.

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

[2] Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 2016).

Figure 1: IRS Risk Management Process



Source: OCRO ERM Program Overview (September 2017).

Our review focused on the identification, assessment, response, and reporting phases of the IT organization's risk management process. The risk identification phase includes processes to support the identification of risks. The purpose of the risk assessment phase is to assess risks in a timely manner once identified. During the risk response phase, appropriate risk responses are considered including risk mitigation and acceptance. Risks with the potential to negatively affect the mission are reported to management during the risk reporting phase.

This review was performed in the IT organization's Applications Development, Cybersecurity, Enterprise Operations, Enterprise Program Management Office, Enterprise Services, Strategy and Planning, and User and Network Services functions, as well as the Customer Account Data

Engine 2, Foreign Account Tax Compliance Act, Integrated Enterprise Portal, Return Review Program, and Web Applications program offices at the New Carrollton Federal Building in Lanham, Maryland, during the period November 2018 through May 2019. 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

Effective risk management can help the IRS, including its IT organization, more securely and effectively administer our Nation's tax system by identifying and mitigating emerging risks before they affect performance. The IT organization is comprised of seven functions, each managed by an Associate Chief Information Officer (ACIO). To assess the IT organization's risk management process, we obtained the 2018 ACIO Risk Registers and selected and reviewed a judgmental sample[3] of three reported risks from each of the following six functions, *i.e.*, 18 total risks: Applications Development, Enterprise Operations, Enterprise Program Management Office, Enterprise Services, Strategy and Planning, and User and Network Services. In addition, we obtained the 2018 Program Risk Registers and selected and reviewed a judgmental sample of three reported risks from each of the following five IT organization programs, *i.e.*, 15 total risks: Customer Account Data Engine 2, Foreign Account Tax Compliance Act, Integrated Enterprise Portal, Return Review Program, and Web Applications. Lastly, we reviewed the Cybersecurity function's Risk-Based Decision (RBD) process by selecting and reviewing a judgmental sample of three accepted risks from the Fiscal Year 2018 RBD Tracker Spreadsheet. The Cybersecurity function uses an RBD Tracker Spreadsheet instead of an ACIO Risk Register to track risks. For our samples, we selected risks that we considered to be of higher significance.

Our review of the IT organization's risk management process found that the functions and programs are identifying, assessing, and reporting risks, but information on risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, is not being captured in sufficient detail to be useful. We also found that accepted unmitigated risks are not being reassessed on a quarterly basis.

Additional Executive Accountability Is Needed for Risk Oversight

We obtained and reviewed the IT organization's 2017 and 2018 Business Unit Risk Registers. The Business Unit Risk Register is prepared once a year by the Information Technology Risk Liaison. Once the Business Unit Risk Register is generated, it is discussed among the ACIOs and the Chief Information Officer before it is shared with the Chief Risk Officer. However, the IT organization's Business Unit Risk Register is not updated throughout the year as the ERM guidance recommends.

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

In December 2017, the Information Technology Risk Liaison drafted an Information Technology Risk Committee Charter. The planned mission of this Committee was to:

- Provide the IT organization executive-level accountability for identifying, managing, and monitoring information technology risks.
- Foster an environment for collaborative and timely risk decisionmaking.
- Provide transparency to risks, including clarity and oversight for significant risks and information technology enterprise risk responses.
- Enable a risk aware culture.

The charter, as presented by IT organization risk management personnel, was created to promote executive accountability over information technology risk management and was given to IT organization management for feedback; however, no further steps were taken to formalize the charter or establish the Information Technology Risk Committee. Without a fully functioning Information Technology Risk Committee that meets to discuss evolving risks periodically throughout the year, there is no assurance that adequate executive management oversight is provided, regular assessments of identified risks are conducted, and significant risks are communicated and timely escalated.

Office of Management and Budget Circular No. A-123 encourages agencies to establish a Risk Management Council, *e.g.*, Information Technology Risk Committee. This council is responsible for ensuring the identification of risks arising from mission and mission-support operations and consideration of those risks as part of the annual strategic review process. In addition, the Government Accountability Office's *Standards for Internal Control in the Federal Government*[4] states that in fostering an effective control environment, management should assess the risks facing the organization as it seeks to achieve its objectives. More specifically, management should identify, analyze, and respond to risks related to achieving the defined objectives for the organization's mission.

Management Action: On April 4, 2019, the Chief Information Officer signed the Information Technology Risk Committee Charter, which incorporated a few minor edits to the mission and other sections of the initially proposed charter. According to the charter, the Information Technology Risk Committee should meet four times a year to review evolving risks for consideration for the IT organization's Business Unit Risk Register. On April 11, 2019, the charter was implemented with the inaugural meeting of the Information Technology Risk

[4] Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

Committee. The Committee is comprised of the Chief Information Officer, Deputy Chief Information Officers, ACIOs, Deputy ACIOs, and the Information Technology Risk Liaison.

Information on Risk Mitigation Plans, Mitigation Activities, and Closure Rationale, As Well As Closure Documentation, Is Not Being Captured in Sufficient Detail to Be Useful

Once a candidate risk is identified and approved by the risk manager, risk coordinators enter the risks into either the Item Tracking Reporting and Control (ITRAC) system or ProSight, depending on which risk management tool the function or program uses. Once identified, function and program personnel assess risks according to risk criticality and potential effect. Risk owners then conduct a thorough analysis of the problems, develop mitigation plans, outline the mitigation activities and timelines, and identify the responsible person(s). Risk owners are responsible for monitoring the progress of the mitigation plans, recommending risks for closure or for escalation to the Chief Information Officer or the ACIOs, as appropriate.

Our review found that the IT organization's functions and programs are identifying, assessing, and reporting risks, but maintained risk information and documentation lacked sufficient detail to enable us to conclude if risks were being appropriately mitigated. The lack of detail is attributed, in part, to some of the IT organization functions using a risk management tool that does not capture essential information. For example, four functions use the ITRAC system to track risks, while two functions use ProSight. There are two important fields captured in the ITRAC system that are not captured in ProSight: closure rationale and risk mitigation activity.

In addition, the ACIO, Strategy and Planning, mandated via a *Risk, Issue, and Action Item Management Directive*, dated June 18, 2018, that all information technology programs and projects should record and maintain risks in the ITRAC system. However, no mention of this requirement was extended to the IT organization functions. By not mandating that the functions use the ITRAC system uniformly, some important risk mitigation information is not being captured.

Further, the ITRAC system User Guide requires detailed descriptions of the mitigation activities and closure rationale. However, none of the function or program risks maintained in the ITRAC system that we reviewed contained enough information for us to evaluate their dispositions properly.

Review of IT organization function risks

Our review of the 18 sampled function risks found that descriptions of the risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, did not include sufficient detail or were not available. We found that not all 18 risks included detailed descriptions of or had descriptions for risk mitigation plans and mitigation activities. For example, the mitigation plan for an Applications Development function risk stated, "Coordinate with delivery partners to align on regression testing timeline for FS 19," without providing any further details. In addition, the listed mitigation activities were not detailed for this risk and there was no closure rationale. Similarly, some of the other risks in the Enterprise Operations, Enterprise Services, and Strategy and Planning functions were completely missing the entirety of information related to the risk mitigation plans, mitigation activities, closure rationale, and closure documentation.

Overall, nine risks did not include closure rationale, four did not include detailed descriptions of closure rationale, and the five remaining risks did not require a closure rationale because they remained candidate risks. Closure documentation was unavailable for seven risks and was not expected for the remaining 11 risks that either were withdrawn or were not closed, *i.e.*, open risks and candidate risks. Figure 2 shows the mitigation summary for the IT organization function risks.

Figure 2: Mitigation Summary for the IT Organization Function Risks

	Mitigation Plan	Mitigation Activities	Closure Rationale	Closure Documentation
Not Detailed	9	7	4	0
Not Available	9	11	9	7
Not Applicable	0	0	5	11

Source: *Treasury Inspector General for Tax Administration summary of risk detail information provided by the IRS and reviewed for our judgmental sample of IT organization function risks (April 2019).*

We also reviewed three sampled RBDs from the Cybersecurity function that represented accepted risks. The Cybersecurity function mitigates its risks through the development of a Plan of Action and Milestones process instead of using the ITRAC system, accepts identified risks through the RBD process, and captures its approved RBDs on the RBD Tracker Spreadsheet. In addition, the Cybersecurity function generally requires all RBDs be documented on a Form 14201, *Risk Acceptance Request*. While only one of the three sampled RBDs was documented on an approved Form 14201, the other two sampled RBDs were not required to have an approved Form 14201.[5] We also found that one of the three Cybersecurity RBDs was properly approved

[5] Use of the Form 14201 was required after January 12, 2018. Two of the three sampled RBDs existed prior to this date.

on the Form 14201 and the other two were included within the approved Security Assessment Report. Because the Cybersecurity function accepted these risks, there was no risk mitigation or risk closure to evaluate.

Review of IT organization program risks

Our review of the 15 sampled program risks found that descriptions of the risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, did not include sufficient detail or did not exist. Although all program risks generally had some basic information, we found that 13 risks did not include detailed descriptions of the risk mitigation plans, 12 risks did not include detailed descriptions of the mitigation activities, 14 risks did not include detailed descriptions of the closure rationale, and 12 risks did not have detailed closure documentation. For example, the mitigation plan for a Foreign Account Tax Compliance Act risk stated, “Prepare Solaris contract extension, create environment, create barrier, remove tiger team,” and the closure rationale provided was “Environments delivered” without providing any further details. In addition, mitigation activities were not detailed for this risk and there were no closure documents available. Overall, mitigation plans were unavailable for two risks, mitigation activities were unavailable for three risks, and closure documentation was unavailable for three risks. One risk did not require a closure rationale because it was reopened. Figure 3 shows the mitigation summary for the IT organization program risks.

Figure 3: Mitigation Summary for the IT Organization Program Risks

	Mitigation Plan	Mitigation Activities	Closure Rationale	Closure Documentation
Not Detailed	13	12	14	12
Not Available	2	3	0	3
Not Applicable	0	0	1	0

Source: Treasury Inspector General for Tax Administration summary of risk detail information provided by the IRS and reviewed for our judgmental sample of IT organization program risks (April 2019).

According to the Government Accountability Office’s *Standards for Internal Control in the Federal Government*, quality information should be appropriate, current, complete, accurate, accessible, and provided on a timely basis, so that management can use the quality information to make informed decisions and evaluate the entity’s performance in achieving key objectives and addressing risks. Management officials stated that descriptions of the risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, should be contained within the ITRAC system risk management tool. However, according to the same officials, closure documentation of approved risk mitigation plans and mitigation actions taken are not required to be uploaded into the ITRAC system although it has the capacity to attach electronic files, *e.g.*, Word and Excel, to an ITRAC record. Without a complete description of the risk mitigation plans, mitigation activities, and closure rationale, as well as closure documentation, it will be more difficult for the IT organization to effectively monitor and manage its outstanding information technology risks.

Recommendations

The Chief Information Officer should require:

Recommendation 1***:*** All IT organization functions (except the Cybersecurity function) to record information technology risks in the ITRAC system.

> ***Management's Response:*** The IRS agreed with this recommendation. The IT organization will reinforce the existing guidance requiring ACIOs to use the ITRAC system, with the exception of the Cybersecurity function.

Recommendation 2: Detailed descriptions of the risk mitigation plans, mitigation activities, and closure rationale be captured and closure documentation be uploaded into the ITRAC system for the IT organization function and program risks, as applicable.

> ***Management's Response:*** The IRS agreed with this recommendation. The IT organization is reinforcing existing policy and guidance that contains detailed directions for capturing risks, descriptions of the risk mitigation plans, mitigation activities, closure rationale, and closure documentation.

Recommendation 3: Periodic review of the risk descriptions and documentation uploaded into the ITRAC system to ensure that the information is appropriate, current, complete, and accurate.

> ***Management's Response:*** The IRS agreed with this recommendation. The IT organization will develop policy that contains guidance on periodic reviews of the risks in the ITRAC system to ensure that risk information is appropriate, current, complete, and accurate.

Accepted Unmitigated Risks Are Not Being Reassessed

When IT organization management has determined that a certain level of risk exposure is acceptable, functional subject matter experts will prepare a Risk Acceptance Form and Tool

(RAFT) for management's review and approval.[6] The IRS developed the RAFT to provide a consistent framework to document business decisions in the context of risk acceptance. According to the IT organization's *Guidelines for Risk Acceptance Form and Tool Completion*, the Business Planning and Risk Management office, within the Strategy and Planning function, is responsible for performing quarterly reviews of IT organization RAFTs. Further, the OCRO requires business units to provide information on accepted risks on a quarterly basis.

We judgmentally selected five IT organization RAFTs for detailed testing.[7] We reviewed the RAFTs for proper approvals and for evidence that management was reviewing and reassessing the accepted risks covered in the RAFTs quarterly. We determined that there were proper management approvals for our sample of the RAFTs. However, management had not reviewed and reassessed all five RAFTs quarterly as required. Accordingly, we expanded our review to include the total population of 20 IT organization RAFTs and observed that 19 had not been reassessed quarterly. For 16 of the RAFTs, the reassessment date was either scheduled or occurred at least one year or more after the RAFT was prepared and IT organization management accepted the risk.

Although there is a timeline established to perform these quarterly review activities throughout the year, we found that the RAFTS were not being reviewed periodically because the Information Technology Risk Liaison's office was relying upon function and program personnel to establish the reassessment dates. Without evidence of regular reviews of the RAFTs, there is limited assurance that the status of the RAFTs is accurate, appropriately reconsidered for mitigation, and properly communicated to the Chief Risk Officer.

Recommendation

Recommendation 4***:*** The Chief Information Officer should reassess risk quarterly, or on a reasonable basis within the year as determined by the risk owner, for all accepted unmitigated risks to ensure that acceptance remains management's preferred response.

> ***Management's Response:*** The IRS agreed with this recommendation. The IT organization will modify processes to ensure that accepted unmitigated risks are reviewed at the appropriate time frames to confirm acceptance remains the acceptable response or whether further action is needed.

[6] The IT organization's Cybersecurity function uses either its RBD process or RAFTs when documenting accepted risks.

[7] The RAFT inventory included 22 total enterprise RAFTs, of which 20 were specifically related to the IT organization.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the effectiveness of the IT organization's risk management process.[1] To accomplish our objective, we:

I. Evaluated the effectiveness of the IT organization's enterprise risk management process.

   A. Obtained and reviewed risk management criteria.

   B. Determined if the IT organization had clearly defined and communicated risk management roles and responsibilities.

   C. Determined how the IT organization identified and tracked risks.

   D. Determined if the IT organization was appropriately mitigating or accepting identified risks and that accepted risks were being reassessed on a quarterly basis.

II. Evaluated the effectiveness of the IT organization functions' risk management process.

   A. Selected a judgmental sample[2] of three risks from the following six 2018 ACIO Risk Registers for detailed testing:

      1. Applications Development.
      2. Enterprise Operations.
      3. Enterprise Program Management Office.
      4. Enterprise Services.
      5. Strategy and Planning.
      6. User and Network Services.

   B. Selected a judgmental sample of three accepted risks from the Cybersecurity function's Fiscal Year 2018 RBD Tracker Spreadsheet.

   C. Determined how each function identified and tracked risks.

   D. Determined if the functions were regularly conducting risk assessments.

[1] See Appendix V for a glossary of terms.
[2] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

E. Determined if the functions were properly mitigating or accepting identified risks.

F. Determined if the functions reported significant risks to the Chief Information Officer.

III. Evaluated the effectiveness of the information technology programs' risk management process.

A. Selected a judgmental sample of three risks from the 2018 Program Risk Registers for the following five information technology programs for detailed testing:

1. Customer Account Data Engine 2.
2. Foreign Account Tax Compliance Act.
3. Integrated Enterprise Portal.
4. Return Review Program.
5. Web Applications.

B. Determined how the program managers identified and tracked risks.

C. Determined whether program managers were regularly conducting risk assessments.

D. Determined whether program managers were properly mitigating or accepting identified risks.

E. Determined whether program managers reported significant risks to the ACIOs.

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: Federal policies and Chief Information Officer policies, procedures, and processes for managing information technology risks. We evaluated these controls by interviewing IT organization personnel, identifying guidance for managing information technology risks, reviewing documents supporting the mitigation of the information technology risks, and independently assessing the risk mitigation process.

Appendix II

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
Mark Carder, Lead Auditor
Denis Danilin, Lead Information Technology Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Chief Risk Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Applications Development
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Program Management Office
Associate Chief Information Officer, Enterprise Services
Associate Chief Information Officer, Strategy and Planning
Associate Chief Information Officer, User and Network Services
Director, Enterprise Audit Management

Appendix IV

Outcome Measures

This appendix presents detailed 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; 18 function risk records and related supporting information that did not include complete descriptions or detailed documentation of the IT organization's risk mitigation efforts (see page 6).

Methodology Used to Measure the Reported Benefit:

We reviewed a judgmental sample[1] of 18 function risk records selected based on the degree of risk significance as determined from our review of the 2018 ACIO Risk Registers. Our review identified that all 18 risks did not include detailed descriptions of or have descriptions for the risk mitigation plans and the mitigation activities. Overall, nine risks did not include closure rationales, four did not include detailed descriptions of the closure rationale, and the five remaining risks did not require a closure rationale because they remained candidate risks.[2] Closure documentation was unavailable for seven risks and not expected for the 11 remaining risks that either were withdrawn or were not closed, *e.g.*, open risks and candidate risks.

This outcome was calculated by determining that for all 18 function risk records we sampled and reviewed, none included complete descriptions or detailed documentation of the IT organization's risk mitigation efforts.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 15 program risk records and related supporting information that did not include complete descriptions or detailed documentation of the IT organization's risk mitigation efforts (see page 6).

[1] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.
[2] See Appendix V for a glossary of terms.

Methodology Used to Measure the Reported Benefit:

We reviewed a judgmental sample of 15 program risk records selected based on the degree of risk significance as determined from our review of the 2018 Program Risk Registers. For the sampled program risks reviewed, we found that 13 risks did not include detailed descriptions of the risk mitigation plans, 12 risks did not include detailed descriptions of the mitigation activities, 14 risks did not include detailed descriptions of the closure rationale, and 12 risks did not have detailed closure documentation. Overall, mitigation plans were unavailable for two risks, mitigation activities were unavailable for three risks, and closure documentation was unavailable for three risks. One risk did not require a closure rationale because it was reopened.

This outcome was calculated by determining that for all 15 program risk records we sampled and reviewed, none included complete descriptions or detailed documentation of the IT organization’s risk mitigation efforts.

Appendix V

Glossary of Terms

Term	Definition
Application	An information technology component of a system that uses information technology resources to store, process, retrieve, or transmit data using information technology hardware and software.
Applications Development	The IT organization function responsible for building, testing, delivering, and maintaining integrated information application systems, *i.e.*, software solutions to support modernized systems and the production environment.
Business Unit	A title for major IRS organizations such as Appeals, the Wage and Investment Division, the Office of Professional Responsibility, and the IT organization.
Candidate Risk	A potential risk or issue that has just been identified, but has not yet been approved or rejected.
Cybersecurity	The IT organization function responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Enterprise Operations	The IT organization function responsible for providing efficient, cost-effective, secure, and highly reliable computing, server, and mainframe services for all IRS business entities and taxpayers.

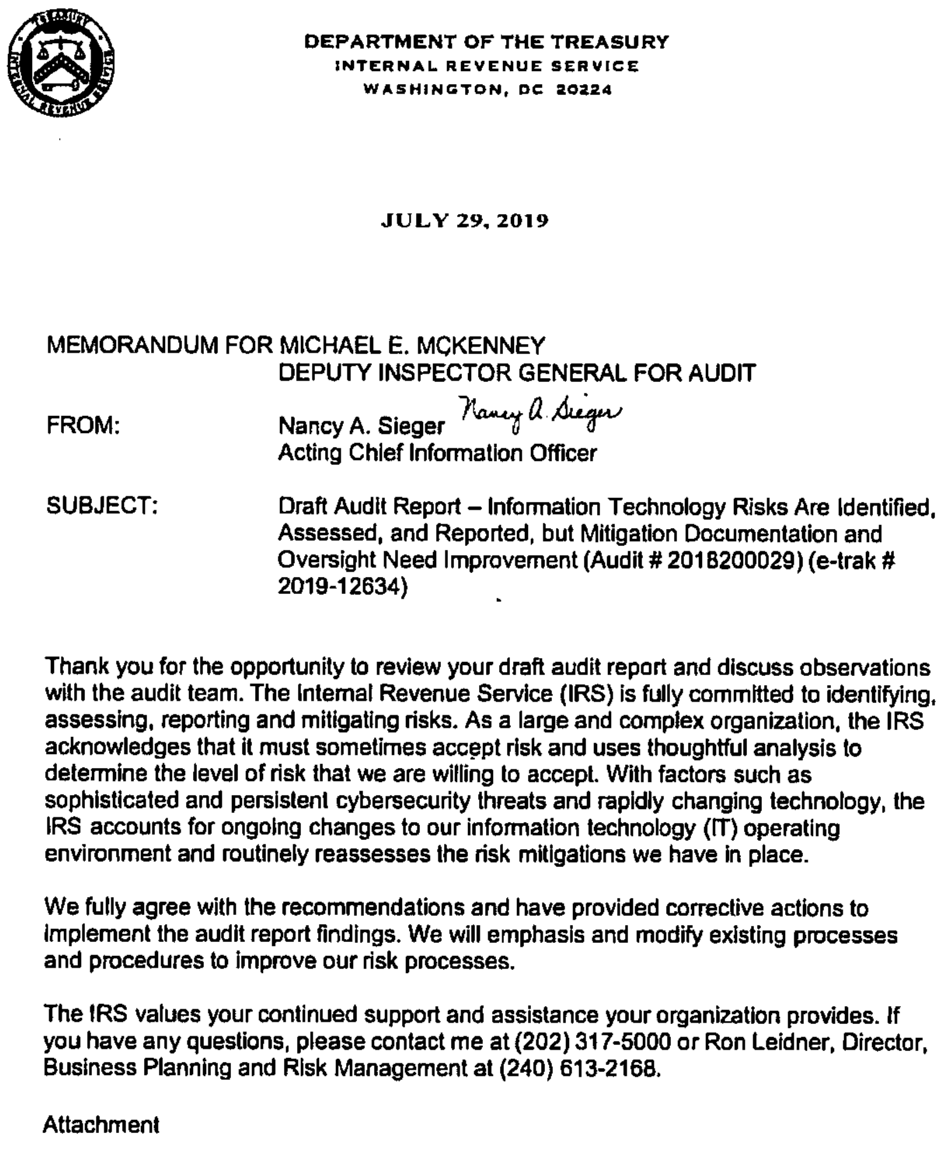
Term	Definition
Enterprise Program Management Office	The IT organization function with the mission to: • Drive program delivery and integration efforts. • Deliver on high-priority program and initiative capabilities. • Mature program management processes, strengthen program management functions, and drive consistency through shared standards and best practices. • Foster a culture of collaboration and integration with business and delivery partners, creating a high-performing workforce and working environment.
Enterprise Risk Management	A process, affected by management and other personnel, designed to identify potential events that may affect the entity, to manage risk to be within the entity's risk appetite, and to provide reasonable assurance regarding the achievement of entity objectives.
Enterprise Risk Management Liaison	Designated officials that serve as ambassadors and champions for risk management and support their business unit leadership in identifying, assessing, and managing risk, that if not mitigated, will undermine the attainment of their business unit's and/or the IRS's goals and mission.
Enterprise Services	The IT organization function that designs and tests enterprise solutions.
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.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by an executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, and support services.

Term	Definition
Item Tracking Reporting and Control System	A customized tool that allows users to submit and update risks, action items, and issues.
Open Risks	Existing risks that are escalated to the Risk Review Board and sorted by status color in the order of red, yellow, or green.
Plan of Action and Milestones Process	The process of planning and identifying the tasks necessary to reduce the risks of each weakness found in an information technology system. It documents the remedial actions taken to address any deficiencies in the security policies and monitors the progress of corrective actions.
ProSight	A database tool designed with specific tracking, reporting, and decision-making features used to monitor projects.
Risk Acceptance	The appropriate risk response when the identified risk is within the organization's risk tolerance. Organizations can accept a risk deemed to be low, moderate, or high depending on particular situations or conditions.
Risk Assessment	The process of determining risks; that is, determining the extent to which an entity is threatened by potential adverse circumstances or events.
Risk-Based Decision	Decision made by individuals responsible for ensuring information security by utilizing a wide variety of information, analysis, assessment, and processes.
Risk Coordinator	A person who facilitates risk assessments at the function and program levels.
Risk Manager	A person who is responsible for risk identification, assessment, mitigation, and reporting.
Risk Owner	A person who is accountable and responsible for formulating the risk response.
Risk Review Board	A group of executives from all organizations that are stakeholders in a program that jointly discuss, make decisions, and provide direction on the risks and issues that have been escalated to this level by each of the partner organizations.

Term	Definition
Security Assessment Report	Information necessary to determine the effectiveness of the security controls employed within or inherited by an information system. Assessment reports are an important factor in determinations of risk.
Senior Risk Advisor	A person who supports the Chief Risk Officer in designing, implementing, and operating the ERM program.
Strategy and Planning	The IT organization function with the mission to facilitate the alignment of information technology and business through strategic planning and financial management practices that offer transparency of overall demand, supply, and the value of information technology investments.
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.
User and Network Services	The IT organization function that supplies and maintains all desktop technology, provides workstation software standardization and security management, inventories data processing equipment, and conducts an annual certification of assets.

Appendix VI

Management's Response to the Draft Report



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

JULY 29, 2019

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger Nancy A. Sieger
Acting Chief Information Officer

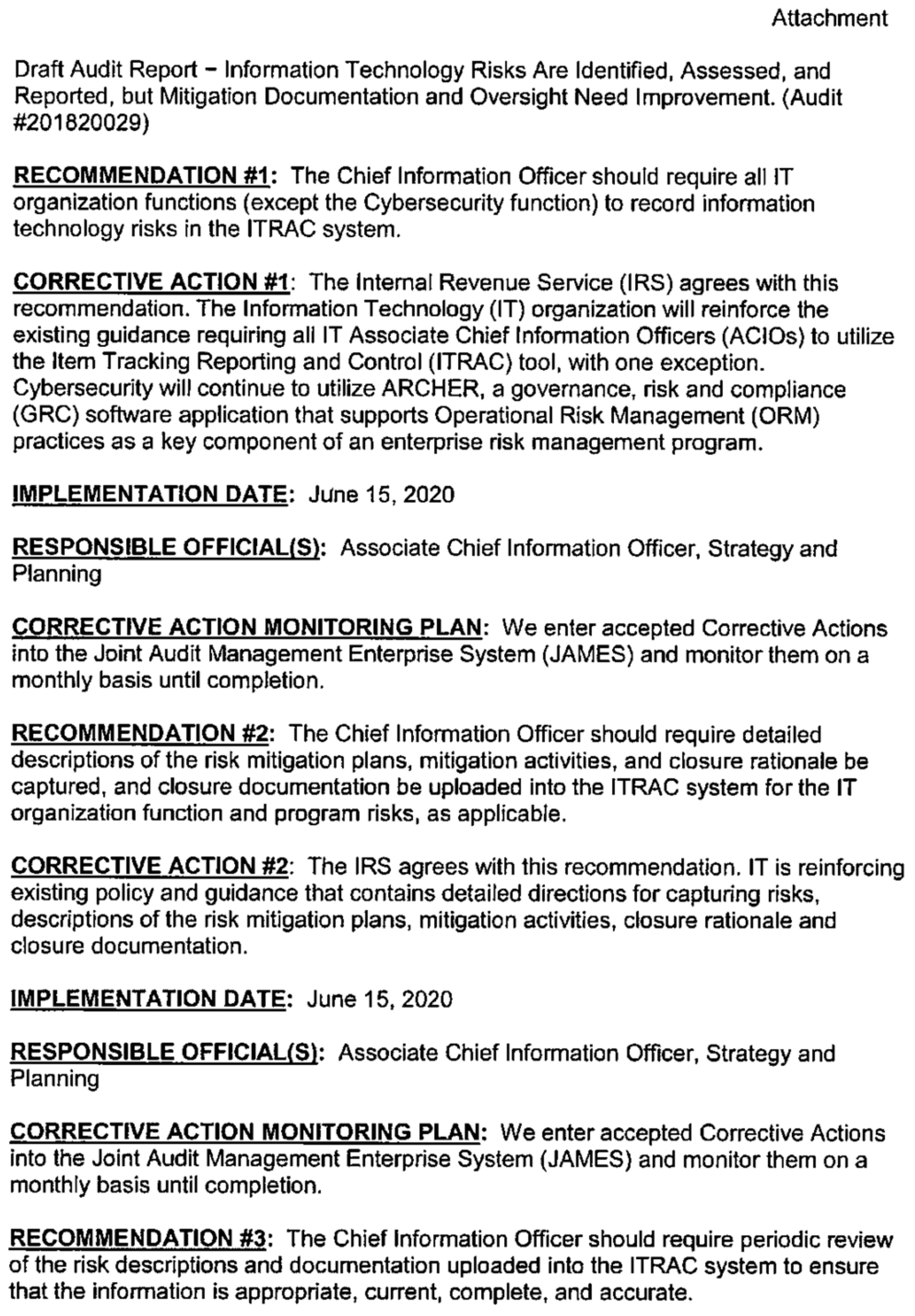
SUBJECT: Draft Audit Report – Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement (Audit # 201820029) (e-trak # 2019-12634)

Thank you for the opportunity to review your draft audit report and discuss observations with the audit team. The Internal Revenue Service (IRS) is fully committed to identifying, assessing, reporting and mitigating risks. As a large and complex organization, the IRS acknowledges that it must sometimes accept risk and uses thoughtful analysis to determine the level of risk that we are willing to accept. With factors such as sophisticated and persistent cybersecurity threats and rapidly changing technology, the IRS accounts for ongoing changes to our information technology (IT) operating environment and routinely reassesses the risk mitigations we have in place.

We fully agree with the recommendations and have provided corrective actions to implement the audit report findings. We will emphasis and modify existing processes and procedures to improve our risk processes.

The IRS values your continued support and assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or Ron Leidner, Director, Business Planning and Risk Management at (240) 613-2168.

Attachment



Attachment

Draft Audit Report – Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement. (Audit #201820029)

RECOMMENDATION #1: The Chief Information Officer should require all IT organization functions (except the Cybersecurity function) to record information technology risks in the ITRAC system.

CORRECTIVE ACTION #1: The Internal Revenue Service (IRS) agrees with this recommendation. The Information Technology (IT) organization will reinforce the existing guidance requiring all IT Associate Chief Information Officers (ACIOs) to utilize the Item Tracking Reporting and Control (ITRAC) tool, with one exception. Cybersecurity will continue to utilize ARCHER, a governance, risk and compliance (GRC) software application that supports Operational Risk Management (ORM) practices as a key component of an enterprise risk management program.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, 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.

RECOMMENDATION #2: The Chief Information Officer should require detailed descriptions of the risk mitigation plans, mitigation activities, and closure rationale be captured, and closure documentation be uploaded into the ITRAC system for the IT organization function and program risks, as applicable.

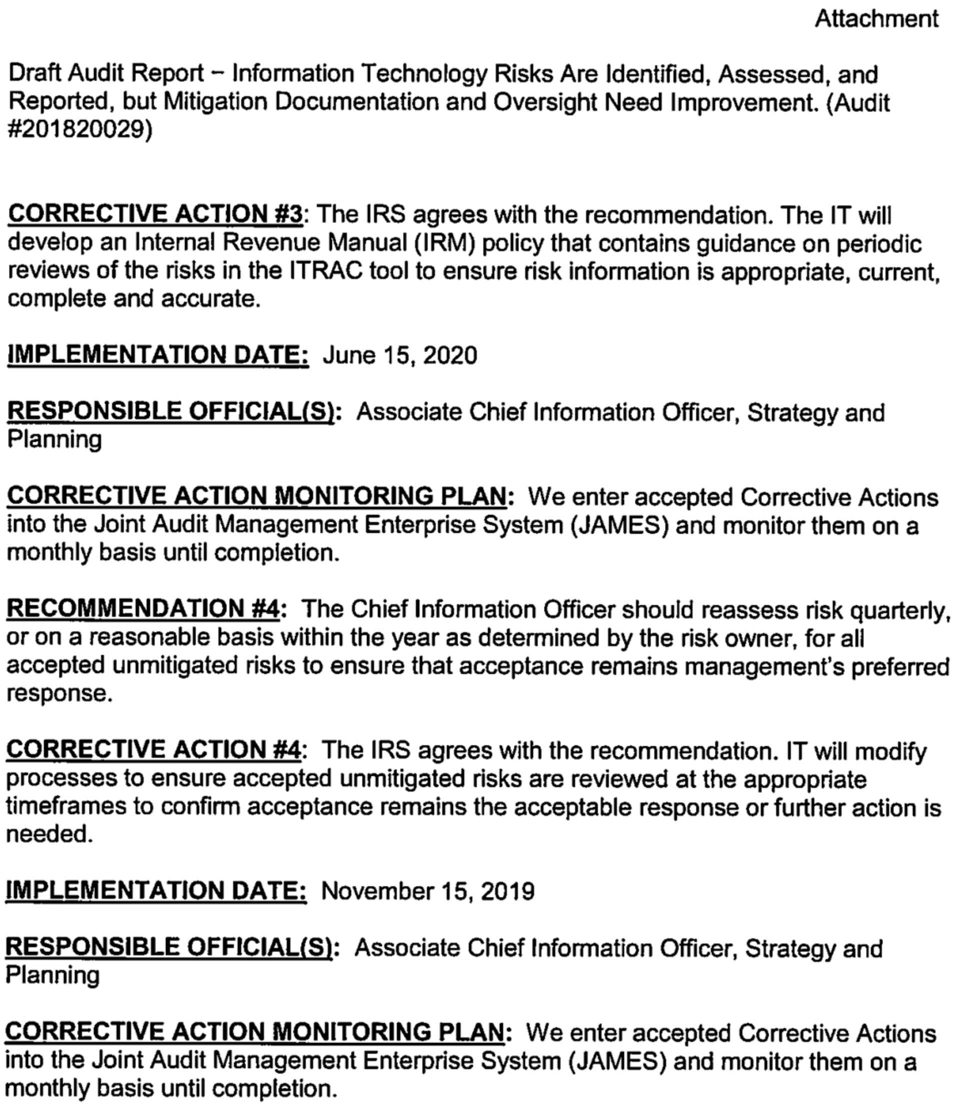
CORRECTIVE ACTION #2: The IRS agrees with this recommendation. IT is reinforcing existing policy and guidance that contains detailed directions for capturing risks, descriptions of the risk mitigation plans, mitigation activities, closure rationale and closure documentation.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, 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.

RECOMMENDATION #3: The Chief Information Officer should require periodic review of the risk descriptions and documentation uploaded into the ITRAC system to ensure that the information is appropriate, current, complete, and accurate.



Attachment

Draft Audit Report – Information Technology Risks Are Identified, Assessed, and Reported, but Mitigation Documentation and Oversight Need Improvement. (Audit #201820029)

CORRECTIVE ACTION #3: The IRS agrees with the recommendation. The IT will develop an Internal Revenue Manual (IRM) policy that contains guidance on periodic reviews of the risks in the ITRAC tool to ensure risk information is appropriate, current, complete and accurate.

IMPLEMENTATION DATE: June 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, 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.

RECOMMENDATION #4: The Chief Information Officer should reassess risk quarterly, or on a reasonable basis within the year as determined by the risk owner, for all accepted unmitigated risks to ensure that acceptance remains management's preferred response.

CORRECTIVE ACTION #4: The IRS agrees with the recommendation. IT will modify processes to ensure accepted unmitigated risks are reviewed at the appropriate timeframes to confirm acceptance remains the acceptable response or further action is needed.

IMPLEMENTATION DATE: November 15, 2019

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, 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.