TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions

September 22, 2014

Reference Number: 2014-20-092

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

THE INTERNAL REVENUE SERVICE DOES NOT ADEQUATELY MANAGE INFORMATION TECHNOLOGY SECURITY RISK-BASED DECISIONS

Highlights

Final Report issued on September 22, 2014

Highlights of Reference Number: 2014-20-092 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Risk-based decisions are made when the IRS wants to make an exception to its own policies and requirements based on suitable justification and a thorough assessment of evident and potential risks. For decisions related to the security of information systems, exceptions are allowed if meeting the requirement is 1) not technically or operationally possible or 2) not cost effective. When risk-based decisions are not made within the established guidelines, the organization may be accepting too much risk related to security of its systems and data. Consequently, taxpayer data may not be secured and may be vulnerable to unauthorized disclosure, which can lead to identity theft. Furthermore, accepted weaknesses may result in security breaches, which can cause network disruptions and prevent the IRS from performing vital taxpayer services, such as processing tax returns, issuing refunds, and answering taxpayer inquiries.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to determine whether the IRS's risk-based decision process provides an effective platform for identifying, assessing, and addressing risks related to information technology projects and systems. This audit is included in TIGTA's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

WHAT TIGTA FOUND

The IRS collects and tracks minimal information about risk-based decisions and does not require supporting documentation about why decisions were made. In addition, information technology risks can be accepted and approved through different processes and may not be known by the Cybersecurity function, which is responsible for the risk-based decision process. TIGTA also found that IRS risk-based decisions are not adequately documented, and information about accepted risks is not centrally located.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer: 1) direct the Cybersecurity function to revise the risk-based decision policy and standard operating procedures to require complete information be collected for all decisions; 2) require all appropriate officials to be trained on what risk-based decision information is required, including justification for the decision based on either technical infeasibility or cost-effectiveness; 3) direct the Cybersecurity function to expand upon its current risk-based decision tracking efforts by maintaining supporting detail in a central repository; and 4) implement a quarterly review of risk-based decision detail to ensure compliance with existing IRS policy and to establish a foundation for risk management of information technology assets.

IRS officials agreed with our recommendations and plan to update policies to clearly state that risk-based decision justification information must be documented to include acceptance due to cost and technical limitations and will add these requirements to training materials. The IRS also plans to enhance the existing repository of risk-based decisions to maintain detailed justification information and will review this detail on a semiannual basis.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 22, 2014

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael E McKenney

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions (Audit #201420006)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) risk-based decision process provides an effective platform for identifying, assessing, and addressing risks related to information technology projects and systems. This audit is included in the Treasury Inspector General for Tax Administration's Fiscal Year 2014 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. This audit is also part of our statutory requirement to annually review the adequacy and security of IRS technology.

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

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 Kent Sagara, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Abbreviations

AO	Authorizing Official
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
RBD	Risk-Based Decision

Background

Risk management can be defined as the identification of possible future events which may affect the ability of an organization to meet its objectives and the implementation of actions to address those events.

In January 2005, the Government Accountability Office identified risk management as an area of concern in the Federal Government. Enterprise risk management[1] is an emerging discipline whereby an organization implements a process across the organization designed to identify potential events that may adversely affect the organization and manage risk to provide reasonable assurance regarding the achievement of organizational objectives. A fundamental concept of enterprise risk management is that it considers activities at all levels of the organization and identifies entity-wide risks. This structure is supported in some agencies, especially those that are larger and more complex, by a dedicated executive and staff specifically responsible for organizational risk management.

Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders and executives address as part of their ongoing risk management responsibilities. Effective risk management requires that organizations operate in highly complex, interconnected environments using state-of-the-art and legacy information systems—systems that organizations depend on to accomplish their missions and to conduct important business-related functions. According to the National Institute of Standards and Technology (NIST), managing risk is a complex, multifaceted activity that requires the involvement of the entire organization—from executives providing the strategic vision and top-level goals and objectives for the organization; to mid-level leaders planning, executing, and managing projects; and to individuals on the front lines operating the information systems supporting the organization's mission and business functions.

When a security risk is discovered and it cannot be easily mitigated, for instance through a configuration change or software upgrade, either a plan must be developed to address the risk or a determination is made to accept the risk. Risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance. Organizations can accept risk deemed to be low, moderate, or high depending on particular situations or conditions. Organizations may accept substantially greater risk due to compelling mission, business, or operational needs. Organizations determine risk by considering the likelihood that known threats exploit known vulnerabilities and the resulting consequences or adverse impacts, *i.e.*, magnitude of harm, if such exploitations occur. Organizations use threat and vulnerability information, together with likelihood and consequences, to quantify the impact to the organization with

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

measureable and relatable outcomes, such as assets, *e.g.*, dollars, resources, information, that could be lost.

Risk tolerance is the level of risk that organizations are willing to accept in pursuit of strategic goals and objectives. Organizations typically make determinations regarding the general level of acceptable risk and the types of acceptable risk with consideration of organizational priorities and trade-offs between:

- Near-term mission or business needs and potential for longer-term mission or business impacts; and
- Organizational interests and the potential impacts on individuals, other organizations, and the Nation.

A risk assessment should document an identified weakness, any risks arising from the weakness, the mitigations which were considered, and the cost and resources required for mitigation. Risk acceptance is necessary when the cost of mitigation is greater than the loss that could be experienced if a weakness was exploited or when mitigation is not technically or operationally feasible. The risk response strategies of organizations empower executives to make risk-based decisions (RBD) compliant with the goals, objectives, and broader organizational perspectives. At the Internal Revenue Service (IRS), the Information Technology (IT) organization's Cybersecurity function provides guidance and oversight for the RBD process. IRS organizations outside of the IT organization can make their own RBDs that do not affect information technology, *i.e.*, business processes, and we did not evaluate any of those processes.

Cybersecurity function officials revised the information technology security RBD process in 2011 and developed a standard operating procedure that details how the IRS can make exceptions to its own information technology security policies based on suitable justification and a thorough assessment of evident and potential risks.[2] At the IRS, only an authorizing official (AO) may explicitly accept risk. The AOs are senior managers or executives who have the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. A system's AO or a designated representative can make an RBD to either allow a system to operate with a weakness unmitigated or partially mitigated, or to take the system out of operation. At the IRS, the AOs are located in various teams such as Enterprise Operations or User and Network Services, depending on system ownership. Information system security officers (ISSO) are responsible for ensuring that the appropriate operational security posture is maintained for an information system or program. The ISSO works in collaboration

[2] The IRS defines the RBD in policy as a decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. IRS RBDs shall not be permanent and, prior to expiring, steps should be taken to either renew the RBD or implement some mitigation to address the weakness. The RBDs expire after one year.

with the information system owner and is the principal advisor to the AO on all matters, technical and otherwise, involving the security of an information system.

According to IRS policy, the only two acceptable reasons for an RBD are:

1. Meeting the requirement is technically or operationally not possible; or
2. Meeting the requirement is not cost-effective.

This review was performed at the IRS IT organization's office in New Carrollton, Maryland, during the period December 2013 through July 2014. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Results of Review

Information Technology Security Risk Is Not Adequately Managed

Information technology security risks are discovered in several ways through different processes. The most common actions that lead to the discovery of weaknesses are security assessments, system configuration scans, and through enterprise continuous monitoring. Weaknesses can also be discovered during development and functional-based activities such as unit testing, regression testing, or integration testing. When risks are identified, agencies can accept the risks or mitigate them. If accepting the risk, decisions should be documented. We found that the IRS tracks basic RBD information, such as any missing control and the date of risk acceptance. This information, however, is not sufficient for risk management of information technology systems.

The RBDs are not adequately documented, and information about accepted risks is not centrally located

According to IRS policy, organizations should thoroughly document a security weakness, the risks arising from the weakness, all mitigations which were considered, the cost of mitigations, and their technical feasibility in order for the AOs to make informed decisions.

We reviewed the various processes by which the IRS accepts information technology risks. At the IRS, risk is identified through the security authorization[3] process for new systems or during a system's annual assessment, and any RBDs made about these vulnerabilities are listed in the system's security plan or within its security assessment report. Security plans and assessment reports are very detailed, lengthy documents that cover a wide spectrum of security information and are not specific to the RBDs. The RBDs are listed in a single table, which is difficult to locate because the plan can be several hundred pages long. When risks are identified outside of the assessment and authorization processes, for example through either policy checker scans or other configuration scans, Cybersecurity function officials created a template that guides staff through documenting the weakness and provides forwarding instructions. The template allocates designated spaces for a description of the weakness, the specific impacted controls, the affected IRS policy, a detailed description of the mitigations considered, and/or mitigating controls applied as justification for risk acceptance. The template also records electronic signatures for each layer of review with comment boxes and forwarding instructions. We found these

[3] Security authorization is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation on an agreed-upon set of security controls.

completed templates contain much more information than what is listed in system security plans or security assessment reports.

According to IRS policy, all RBDs are required to be tracked in an RBD library. However, our analysis determined that the RBDs are neither supported nor adequately tracked in the spreadsheet Cybersecurity function officials refer to as their library. The RBD library is a spreadsheet of identified accepted risks consisting of about 10 columns, and is not a repository of detailed information nor an adequate risk register that the IRS could use to manage risk enterprise-wide. Risks identified in this spreadsheet are not supported by detailed technical documentation or cost estimates that properly support the decision to forego implementation of the control and mitigate the risk. The RBDs are dated and listed with only minimal detail. Even when the previously described template is used to thoroughly document an RBD identified during a policy checker scan, a link to that detailed documentation is not provided in the RBD library. No hyperlinks in the library exist which could be used as a management information system to provide supporting documentation and used as a centralized resource for enterprise-wide risk assessment or analysis.

Furthermore, the RBD library is not a complete list of all RBDs throughout the agency. For example, the spreadsheet has no information about information technology development projects. The NIST recognizes that risks are accepted during development, but the IRS does not centrally track any risks in systems that are not yet deployed. Also, the IRS does not track risks found in non-major systems.

In September 2011, we reported that the IRS IT organization was in the early stages of developing a formalized, integrated risk management framework to manage information technology risks.[4] Specifically, IT organization management implemented a dedicated group, headed by a senior executive, to specifically focus on managing risks applicable to IRS information technology. As part of our review, we attempted to contact the IRS Enterprise Risk Management Executive, but at the time of our review the position was vacant. We interviewed the Director, Business Planning and Risk Management, to determine his team's roles and responsibilities in the RBD process. He leads and executes matters related to requirements and risk management issues that could affect information technology operations. He stated that he wants to try to establish a repository for the RBDs with supporting documentation that could be used to manage risk at the enterprise level.

According to the NIST, the culture[5] of an organization influences the willingness of personnel to communicate potential threat and vulnerability information, which ultimately affects the quality and quantity of the threats and vulnerabilities identified. The organization's culture informs and

[4] Treasury Inspector General for Tax Administration, Ref. No. 2011-10-096, *Risk Management Efforts Could Be Improved With Clearly Defined Procedures and Expanded Information Sharing* (Sept. 2011).

[5] Organizational culture describes the way things are done in organizations and can explain why certain things occur—and culture refers to the values, beliefs, and norms that influence the behaviors and actions of the senior leaders and executives and individual members of organizations.

even, to perhaps a large degree, defines that organization's risk management strategy. At a minimum, when an expressed risk management strategy is not consistent with that organization's culture, it is likely that the strategy will be difficult if not impossible to implement. Recognizing and addressing the significant influence culture has on risk-related decisions of senior leaders and executives within organizations can be crucial to achieving effective management of risk. According to the NIST, implementing an effective risk management program may well represent a significant organization-wide change aligning the people, processes, and culture within the organization with the new or revised organizational goals and objectives, the risk management strategy, and the communication mechanisms for sharing risk-related information among entities.

Information technology RBDs affect the IRS's overall enterprise risk management program

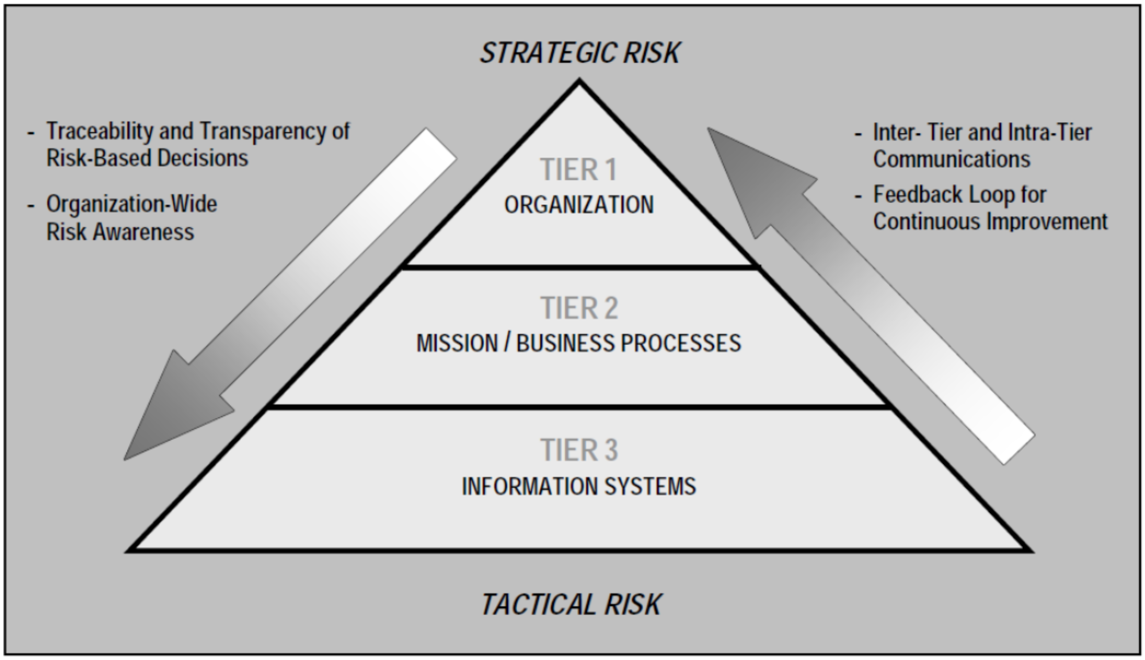
According to the NIST, several benefits can be derived from enterprise-wide risk management. Goals for risk management across an organization include:

- A strategic alignment of risk management decisions with missions and business functions.
- Execution of risk management processes to assess, respond to, and monitor risk to organizational operations and assets, individuals, and the Nation.
- Effective and efficient allocation of risk management resources.

Enterprise-wide risk management can deliver value by optimizing risk management investments in support of organizational objectives. When implementing enterprise-wide risk management, a key component is oversight for risk management activities to ensure consistent and effective RBDs.

Monitoring the effectiveness of risk management activities is a key component of a properly functioning risk management process. According to the NIST, senior leaders and executives have historically had a very narrow view of information security either as a technical matter or in a stovepipe that was independent of organizational risk and the traditional management and lifecycle processes. The NIST concluded that this extremely limited perspective often resulted in inadequate consideration of how information security risk, like other organizational risks, affects the likelihood of organizations successfully carrying out their missions and business functions. Figure 1 shows that risk management should be carried out as a holistic, organization-wide activity that addresses risk from the strategic level to the tactical level, ensuring that the RBDs are integrated into every aspect of the organization.

Figure 1: Multitiered Organization-Wide Risk Management


STRATEGIC RISK
- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness
- Inter- Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement
TIER 1
ORGANIZATION
TIER 2
MISSION / BUSINESS PROCESSES
TIER 3
INFORMATION SYSTEMS
TACTICAL RISK

Source: NIST Special Publication 800-39, Managing Information Security Risk (March 2011).

As examples based on Figure 1, Tier 1 monitoring activities might include ongoing threat assessments and how changes in the threat space may affect lower-tier activities, including enterprise architectures (with embedded information security architectures) and organizational information systems. Tier 2 activities might include analyses of new or current technologies considered for future use to identify exploitable weaknesses or deficiencies in those technologies that may affect mission success. Tier 3 activities focus on information systems and might include automated monitoring of standard configuration settings for information technology systems, vulnerability scanning, and ongoing assessments of security controls.

Because the RBDs are not consistently documented, reviewed, or maintained centrally, IRS management lacks the ability to adequately manage information technology RBDs, which ultimately affects the IRS's ability to manage enterprise risk. For example, individual AOs at the information system level (Tier 3) may understand why a decision was made, but if that decision is not sufficiently documented alongside other mitigations considered and weighed against the costs of mitigation, officials in different business units will be unable to use or leverage that information to address security vulnerabilities. According to the NIST, the activities at Tier 3 should provide essential feedback upward through the organization. For example, new vulnerabilities discovered in an information system may have systemic implications that extend organization-wide. Those same vulnerabilities may trigger changes to the enterprise architecture and embedded information security architecture or may require an adjustment to the organizational risk tolerance.

According to the NIST, leaders must recognize that explicit, well-informed RBDs are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure. IRS Cybersecurity function executives responsible for information technology risk at the agency stated they are briefed on all RBDs and are aware of all the risks in deployed information systems. However, we found that these executives did not know why decisions were made, whether other alternatives or mitigation solutions might exist, or how much these solutions might cost. We found no oversight of the RBD process that includes checking the rationale and analysis for the decisions to ensure that they are only being made for one of the two allowable reasons per IRS policy: technical infeasibility or cost-effectiveness.

Because we could not find detailed assessment information contained within the RBD library itself, we had to request additional information from the IRS in order to ascertain the nature of the RBD decision as well as supporting artifacts on the decisions made. After limited success in requesting source documents from the Cybersecurity function, we decided to contact the AOs and their security counterparts to determine whether they had any supporting information for recent moderate- and high-risk RBDs.

We received inconsistent and incomplete information from the AOs and the security officers. Most gave us a copy of their system's security plan, which is limited in support and provides no reasoning or rationale about why the decision was made to not fix the vulnerability. With the exception of one AO, none provided cost estimates or technical considerations as justification for the RBDs, and we obtained no evidence that any cost-benefit analyses were conducted prior to accepting the risks.

As an illustration of the RBDs made, we found one platform where the AO identified 27 security controls as RBDs. These RBDs included the lack of secure communications, the inability to detect and protect against unauthorized changes to software and information, and the inability to uniquely identify users and enforce inactivity lockout controls. Because we received no supporting analysis documents, we have no assurance that these RBDs as well as the level of risk accepted were justified and appropriate.

With insufficient oversight of the RBD process and limited information about why decisions are being made, IRS systems and data are at risk of breach by insider threats and could potentially result in wasted resources through fraud or collusion with contractors and software vendors. Documenting the costs of risk remediation becomes more important when funds are limited and vulnerabilities are higher risk. Agencies cannot make smart decisions about where to spend limited funds without estimated mitigation costs and other relevant technical information.

Recommendations

The Chief Technology Officer should:

Recommendation 1: Revise the RBD policy and standard operating procedures to require complete information to be collected for every information technology RBD by completing the template already being used by some staff in limited situations.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity function will ensure that the enterprise risk acceptance and RBD standard operating procedures clearly state that justification information must be documented when information technology security risks are accepted, including information if the acceptance is due to cost and technical limitations.

Recommendation 2: Require all AOs to be trained on the information required for the RBDs, including justification for the RBD based on either technical infeasibility or cost-effectiveness, and include estimates of mitigation costs for the latter.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity function will add requirements related to acceptance of the RBDs to already existing briefing materials which are provided to the AOs annually.

Recommendation 3: Expand upon current RBD tracking efforts by maintaining collected RBD detail in a central repository.

> **Management's Response:** The IRS agreed with this recommendation. The Cybersecurity function will enhance the current information technology security RBD central repository form to maintain detailed justification information.

Recommendation 4: Implement a quarterly review of RBD detail to ensure compliance with existing IRS policy.

> **Management's Response:** The IRS agreed with this recommendation. Given the IRS's established RBD processes, the Cybersecurity function will review the RBD detail on a semiannual basis. The Chief Technology Officer will be presented with a summary-level review on an annual basis to ensure compliance with existing IRS policy.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether the IRS RBD[1] process provides an effective platform for identifying, assessing, and addressing risks related to information technology projects and systems. To accomplish our objective, we:

I. Determined which functions at the IRS have designated roles and responsibilities for information technology RBDs, and whether related processes and practices allow for effective risk coordination across the agency.

   A. Interviewed Cybersecurity function officials to obtain a detailed description of RBD processes they manage and track.

   B. Interviewed Business Planning and Risk Management leadership to determine their roles and responsibilities and whether they track, manage, contribute to, coordinate, or influence any RBD process.

   C. Evaluated whether any redundancies or conflicts in roles and responsibilities exist for RBD processes.

   D. Determined which function is responsible for maintaining and updating the RBD library.

II. Reviewed the various processes and procedures for identifying, initiating, evaluating, approving, and documenting the RBDs.

   A. Reviewed and analyzed the various policies and procedures that state what is to be done when a security risk is identified and an RBD is initiated, and how RBDs are evaluated and approved.

   B. Determined whether there are other processes which may fall outside the designated IRS policies and procedures that allow the IRS to accept risk, and whether these are reconciled and coordinated with those documented through established RBD processes.

   C. Determined whether any systems were taken offline due to analysis conducted for a RBD.

III. Evaluated the risks accepted by the IRS to determine whether approved RBDs are adequately supported and appropriately tracked and monitored in the RBD library.

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

A. Evaluated the risks accepted by the IRS by reviewing all recent high- and moderate-risk RBDs that are tracked in the RBD library.

   1. Determined whether a cost-benefit analysis was performed to justify the decision.

   2. Determined whether costs of the RBDs are captured and controlled in the RBD library system.

   3. Determined whether a detailed technical description of feasibility was included.

B. Determined whether the RBD library is used to efficiently track and monitor all RBDs in a centralized management information system.

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: NIST guidelines and IRS policies related to risk assessment and RBD decisionmaking. We evaluated these controls by conducting interviews and meetings with Cybersecurity function management and staff. We also reviewed RBD supporting documentation.

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph F. Cooney, Audit Manager
Jena Whitley, Lead Auditor
George L. Franklin, Senior Auditor
Mary Jankowski, Senior Auditor

Appendix III

Report Distribution List

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

Appendix IV

Glossary of Terms

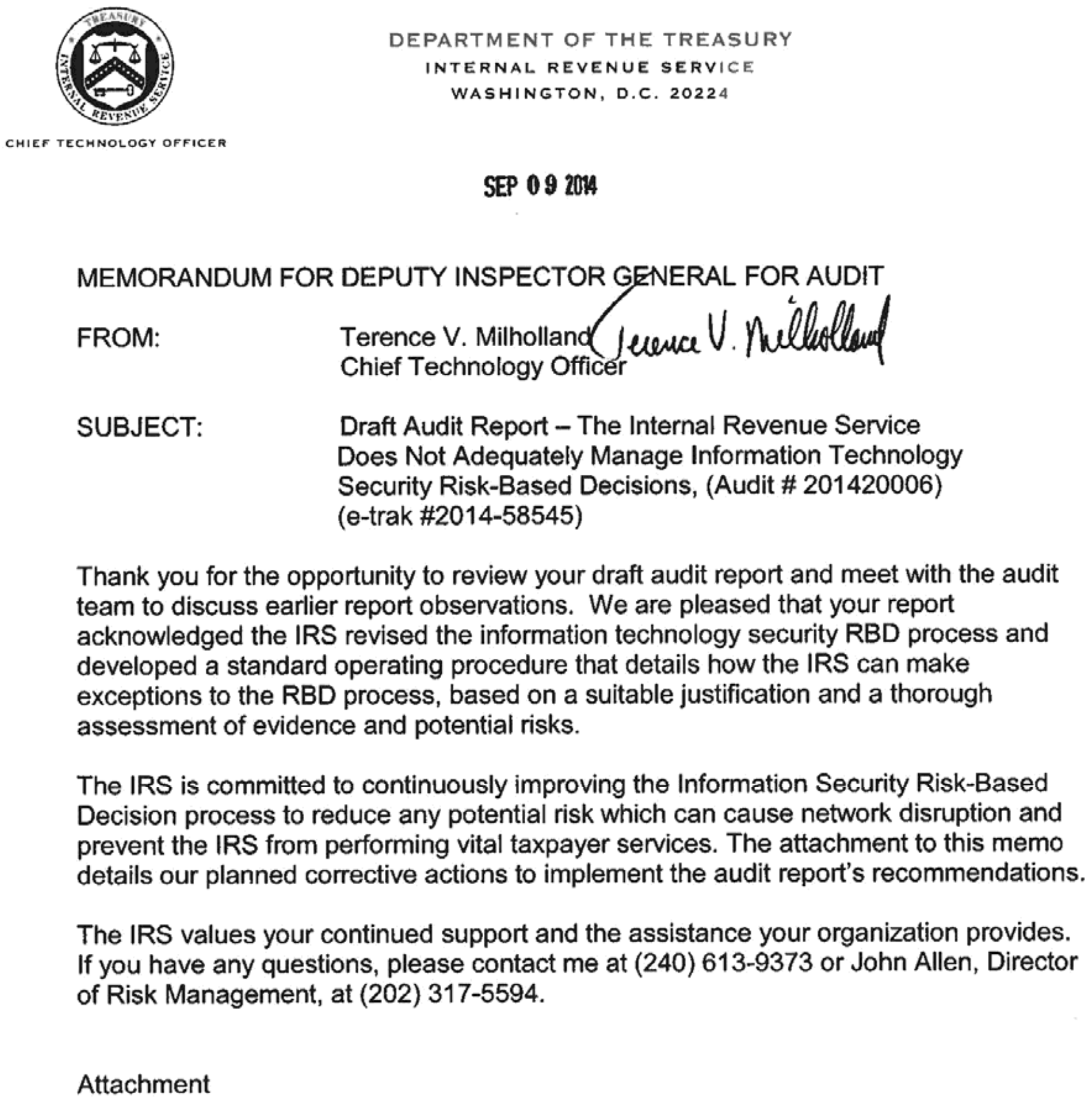
Term	Definition
Authorizing Official	The official accountable for the security risks associated with information system operations and with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Cybersecurity	A function within the IRS IT organization 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	A function within the IRS IT organization responsible for providing efficient, cost-effective, secure, and highly reliable computing, server, and mainframe services for all IRS business entities and taxpayers.
Enterprise Risk Management	The methods and processes used by an enterprise to manage risks to its mission and to establish the trust necessary for the enterprise to support shared missions. It involves the identification of mission dependencies on enterprise capabilities, the identification and prioritization of risks due to defined threats, the implementation of countermeasures to provide both a static risk posture and an effective dynamic response to active threats, and the assessment of enterprise performance against threats and adjustment of countermeasures as necessary.
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.

Term	Definition
Information System Security Officer	The individual assigned responsibility by the senior agency information security officer/chief information security officer, authorizing official, management official, or information system owner for ensuring that the appropriate operational security posture is maintained for an information system or program.
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 or information by an executive agency. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.
National Institute of Standards and Technology	The NIST, under the Department of Commerce, is responsible for developing standards and guidelines for providing adequate information security for all Federal Government agency operations and assets.
Risk Acceptance	The appropriate risk response when the identified risk is within the organizational risk tolerance. Organizations can accept 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 assessment for information system-related security risks includes assessment of the susceptibility to adverse impacts through information, *e.g.*, consideration of the dependence on information, the vulnerabilities in mission and business processes, and the effectiveness of risk mitigations, and assessment of the threat environment with regard to causing such impacts.
Risk-Based Decision	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes.

Term	Definition
Risk Tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
Security Authorization	The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Stovepipe	A structure which largely or entirely restricts the flow of information within the organization through lines of control, inhibiting or preventing cross-organizational communication.
System Security Plan	Formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.
Threat	Any circumstance or event with the potential to adversely affect agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, or denial of service.
User and Network Services	A function within the IRS IT organization that supplies and maintains all desk-side (including telephone) technology, provides workstation software standardization and security management, inventories data-processing equipment, conducts annual certification of assets, and other services.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Appendix V

Management's Response to the Draft Report



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

CHIEF TECHNOLOGY OFFICER

SEP 09 2014

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

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

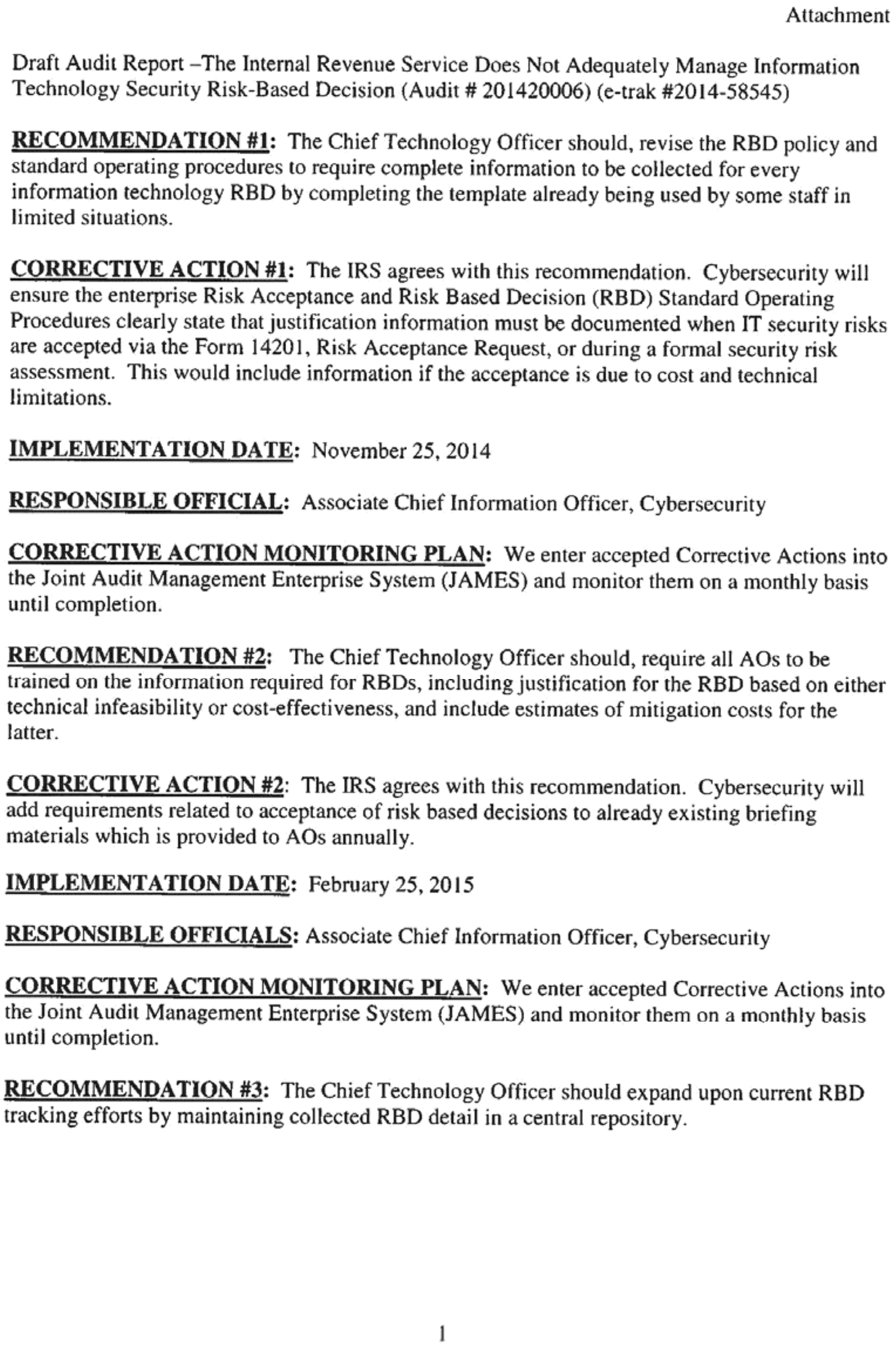
SUBJECT: Draft Audit Report – The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decisions, (Audit # 201420006) (e-trak #2014-58545)

Thank you for the opportunity to review your draft audit report and meet with the audit team to discuss earlier report observations. We are pleased that your report acknowledged the IRS revised the information technology security RBD process and developed a standard operating procedure that details how the IRS can make exceptions to the RBD process, based on a suitable justification and a thorough assessment of evidence and potential risks.

The IRS is committed to continuously improving the Information Security Risk-Based Decision process to reduce any potential risk which can cause network disruption and prevent the IRS from performing vital taxpayer services. The attachment to this memo details our planned corrective actions to implement the audit report's recommendations.

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (240) 613-9373 or John Allen, Director of Risk Management, at (202) 317-5594.

Attachment



Attachment

Draft Audit Report –The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decision (Audit # 201420006) (e-trak #2014-58545)

RECOMMENDATION #1: The Chief Technology Officer should, revise the RBD policy and standard operating procedures to require complete information to be collected for every information technology RBD by completing the template already being used by some staff in limited situations.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. Cybersecurity will ensure the enterprise Risk Acceptance and Risk Based Decision (RBD) Standard Operating Procedures clearly state that justification information must be documented when IT security risks are accepted via the Form 14201, Risk Acceptance Request, or during a formal security risk assessment. This would include information if the acceptance is due to cost and technical limitations.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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 Technology Officer should, require all AOs to be trained on the information required for RBDs, including justification for the RBD based on either technical infeasibility or cost-effectiveness, and include estimates of mitigation costs for the latter.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation. Cybersecurity will add requirements related to acceptance of risk based decisions to already existing briefing materials which is provided to AOs annually.

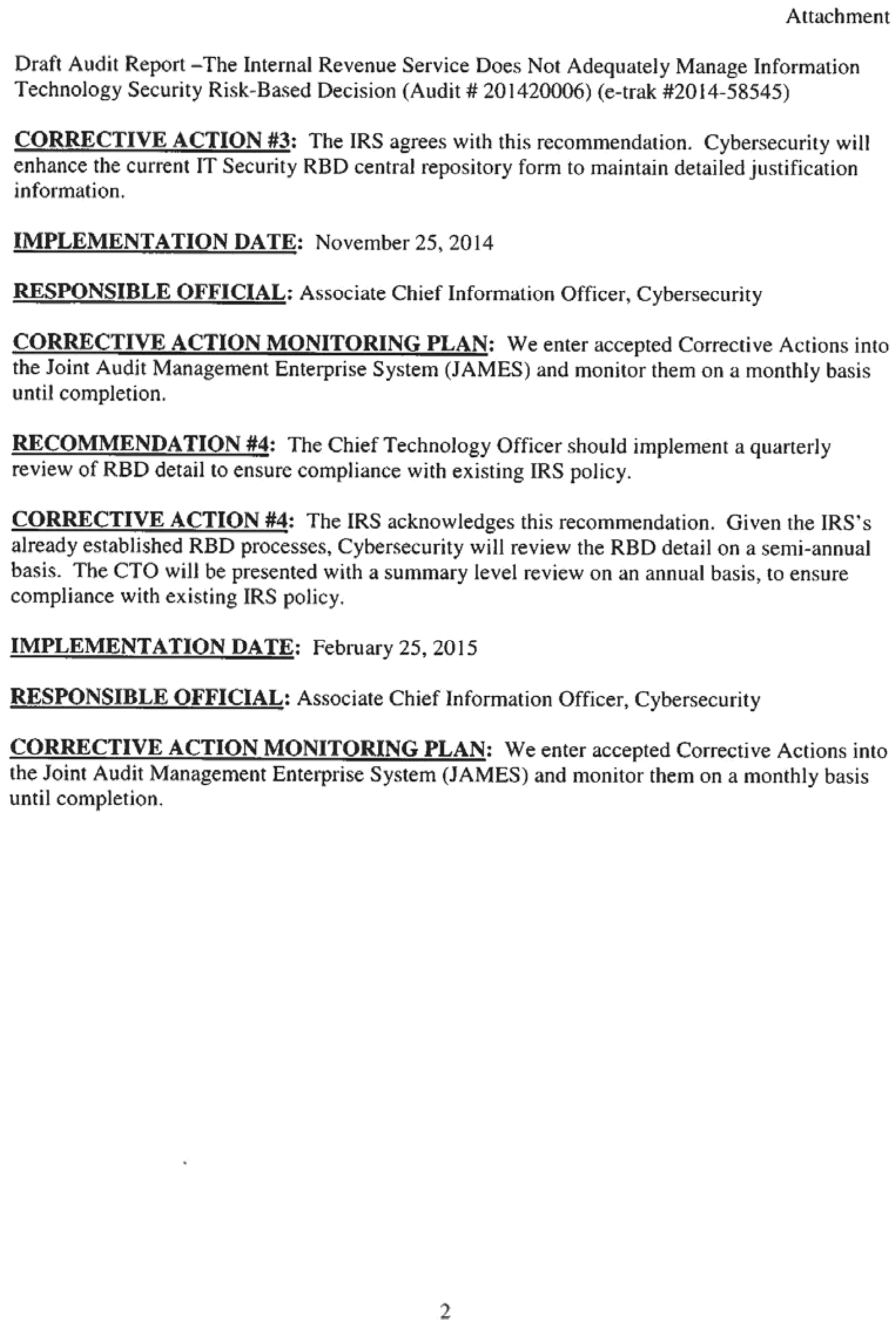
IMPLEMENTATION DATE: February 25, 2015

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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 Technology Officer should expand upon current RBD tracking efforts by maintaining collected RBD detail in a central repository.

1



Attachment

Draft Audit Report –The Internal Revenue Service Does Not Adequately Manage Information Technology Security Risk-Based Decision (Audit # 201420006) (e-trak #2014-58545)

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. Cybersecurity will enhance the current IT Security RBD central repository form to maintain detailed justification information.

IMPLEMENTATION DATE: November 25, 2014

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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 Technology Officer should implement a quarterly review of RBD detail to ensure compliance with existing IRS policy.

CORRECTIVE ACTION #4: The IRS acknowledges this recommendation. Given the IRS's already established RBD processes, Cybersecurity will review the RBD detail on a semi-annual basis. The CTO will be presented with a summary level review on an annual basis, to ensure compliance with existing IRS policy.

IMPLEMENTATION DATE: February 25, 2015

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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.