TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes

September 10, 2024

Report Number: 2024-200-047

TIGTACommunications@tigta.treas.gov | www.tigta.gov

Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes

Final Audit Report issued on September 10, 2024 **Report Number 2024-200-047**

Why TIGTA Did This Audit

The Federal Risk and Authorization Management Program (FedRAMP) Security Threat Analysis Report is an IRS created document that contains a systematic analysis and assessment of a Cloud Service Provider in the FedRAMP. The report includes which cloud controls failed the most recent assessment, probable threat characteristics, and the most likely attack vectors.

Preparing the Security Threat Analysis Reports and performing continuous monitoring are important activities that help ensure that cloud system security is assessed periodically and monitored.

This audit was initiated to determine whether Security Threat Analysis Reports were prepared and if continuous monitoring efforts were adequate to ensure the security of IRS cloud systems.

Impact on Tax Administration

Governmentwide mandates require Federal agencies to expand the use of shared services to enable broader use and adoption of cloud computing. When an application hosted in the cloud has unidentified internal control deficiencies or security weaknesses that are not being monitored it can potentially lead to disclosure of sensitive data.

What TIGTA Found

The IRS was not maintaining appropriate separation of duties for certain roles related to cloud systems. The IRS did not follow guidance meant to prevent conflicts of interest, increasing the risk of erroneous and inappropriate actions. Specifically, 35 (70 percent) of 50 cloud systems reviewed had the same individual filling the System Owner and Authorizing Official roles. TIGTA also identified a cloud system that was operating in a production environment despite not having the required security documentation, including an approved Authorization-to-Operate memorandum.

Processes to maintain cloud systems' security were not effective. Information System Security Officers were not preparing required continuous monitoring executive summary reports. Specifically, summary reports for 11 (22 percent) of 50 cloud systems reviewed were not prepared every month as required. Summary reports for the remaining 39 (78 percent) of 50 cloud systems were prepared as required. As of March 2024, the Information System Security Officers are now preparing summary reports for 6 of 11 cloud systems that did not have summary reports previously.

In addition, 31 (69 percent) of the 45 cloud systems reviewed were missing the trackable Plan of Action and Milestones weakness identification number on the summary report (five cloud systems reviewed did not have a summary report). Further, security documents were missing approvals or were not properly approved within the Department of the Treasury data repository. Specifically, the repository was missing five (10 percent) of the 50 cloud systems' Authorization-to-Operate memorandums.

Finally, 15 (30 percent) of 50 cloud systems were missing required FedRAMP Security Threat Analysis Reports. These reports contain a systemic analysis and assessment of a cloud system's security, including that of the Cloud Service Provider hosting the system.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer ensure that: 1) separation of duty controls reflect guidance and require that all cloud systems have a unique System Owner and Authorizing Official; 2) an Authorization-to-Operate memorandum is approved for the system to remain in production; 3) summary reports are timely created; 4) procedures are updated; 5) management approvals are consistent and documented; and 6) the Cloud Security Assessment and Authorization process is completed annually.

The IRS agreed with four recommendations and plans to ensure separation of duty controls reflect guidance; the system obtains authorization; that summary reports are timely created; and that management approvals are documented. The IRS disagreed with two recommendations stating its weakness summary reporting is sufficient without unique identifiers and that cloud security assessments are completed in accordance with existing procedures.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 10, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Danny R. Verneuille
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes
(Audit No.: 2024200003)

This report presents the results of our review to determine whether the Federal Risk and Authorization Management Program Security Threat Analysis Reports (FSTAR) were prepared and if continuous monitoring efforts were adequate to ensure the security of the Internal Revenue Service's (IRS) cloud systems. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data and IRS Resources.*

Management's complete response to the draft report is included as Appendix III. If you have any questions, please contact me or Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Background

Governmentwide mandates require Federal agencies to expand the use of shared services to enable broader use and adoption of cloud computing.[1] Cloud computing is defined as the delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet to offer faster innovation, flexible resources, and economies of scale. The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. Government program to standardize how the Federal Information Security Modernization Act of 2014 (FISMA) applies to cloud computing services.[2] The FedRAMP mission is to promote the adoption of secure cloud services across the Government by providing a standardized approach to security and risk assessment. FISMA focuses on improving oversight of Federal information security programs and facilitating progress in correcting agency information security weaknesses. When an application hosted in the cloud has unidentified internal control deficiencies or security weaknesses that are not being monitored it can potentially lead to disclosure of sensitive data.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring of cloud-based services. To be a FedRAMP authorized Cloud Service Provider (CSP), a CSP must have their security controls reviewed by an independent third party and the results of the review incorporated into an authorization package. The FedRAMP Program Management Office reviews the authorization package to determine whether the CSP meets the FedRAMP requirements to be an authorized CSP that can be listed on the FedRAMP marketplace. The FedRAMP marketplace is the site that agencies use to research cloud services that meet their organizational requirements. The initial authorization package is updated annually by having a third-party assessment organization evaluate the status of the CSP's internal controls. The updated FedRAMP package is made available for review by agencies that are considering contracting with that CSP. Leveraging existing authorizations for future contracts is one of the primary advantages of the FedRAMP program. Federal agencies can contract with any CSP listed on the marketplace and can review the latest authorization package for that CSP prior to entering into a contract.

The FedRAMP also provides guidance related to continuous monitoring of cloud services by contracting agencies. The Internal Revenue Service's (IRS) cloud continuous monitoring program is meant to ensure that ongoing authorization activities are supported, and security-related information collected during continuous monitoring is used to maintain security authorization packages. The assigned cloud Information System Security Officer (ISSO) for each system performs the IRS monitoring activities. In addition, the CSP must monitor its own security controls, assess them on a regular basis, and demonstrate that the security posture of its service is continuously acceptable. The third-party assessment organization is responsible for

[1] Governmentwide mandates include the Federal Cloud Computing Strategy ("Cloud First" and "Cloud Smart") (Feb. 2011, and June 2019, respectively); Office of Management and Budget, Memoranda M-16-19, *Data Center Optimization Initiative* (Aug. 2016), and M-19-19, *Update to Data Center Optimization Initiative* (June 2019); and Executive Orders 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 2017), and 14028, *Improving the Nation's Cybersecurity* (May 2021).

[2] 44 U.S.C. § 3551, et seq. (2018). See Appendix IV for a glossary of terms.

independently verifying and validating the controls implemented and the test results for the CSP.

The ISSOs ensure that applicable cybersecurity policies are implemented for their assigned systems, which includes monitoring compliance with system security policies and providing guidance and recommendations to correct deficiencies. The ISSO serves as the principal advisor to the system Authorizing Official (AO) and System Owner on all matters involving the cybersecurity of the system.

The FedRAMP Security Threat Analysis Report (FSTAR) is an IRS created document that contains a systematic analysis and assessment of the CSP's FedRAMP package, including which cloud controls failed the most recent assessment, probable threat characteristics, and the most likely attack vectors. Preparing an FSTAR and performing continuous monitoring are important activities that help ensure that cloud system security is assessed periodically and monitored. An FSTAR is required when new IRS programs, projects, or information systems intend to acquire a FedRAMP authorized cloud solution or when existing business units intend to introduce a FedRAMP authorized cloud service into IRS boundaries. The IRS is also required to update the FSTAR annually once an initial Authorization-to-Operate (ATO) has been granted.

Results of Review

The IRS Did Not Maintain Appropriate Separation of Duties

We identified 50 IRS cloud systems present on the Treasury FISMA Inventory Management System (TFIMS), *i.e.*, the Department of the Treasury official FISMA data repository, as of November 9, 2023, and reviewed specific information for each system. We determined that 35 (70 percent) of the 50 cloud systems reviewed had the same individuals assigned as either the AO or the AO Designated Representative and System Owner. The remaining 15 (30 percent) of the 50 cloud systems reviewed demonstrated appropriate separation of duty with different individuals assigned as the AO or the AO Designated Representative and System Owner.

National Institute of Standards and Technology (NIST) guidelines recommend that organizations ensure that there are no conflicts of interest when assigning the same individual to multiple risk management roles.[3] For example, AOs or AO Designated Representatives cannot occupy the role of System Owner or common control provider for systems or common controls they are authorizing.

IRS management stated that it allowed the same individual to occupy both System Owner and AO or AO Designated Representative roles because there was no IRS policy statement that specifically prevented the roles from being occupied by the same person. After this issue was brought to management's attention, IRS officials stated it will review the NIST guidance and work to ensure that updates are made as appropriate to have different individuals occupy these roles.

[3] NIST, Special Publication 800-37, Rev 2, *Risk Management Framework for Information Systems and Organizations* (Dec. 2018).

Insufficient separation of duties elevates the risk of both erroneous and inappropriate actions whether deliberate or unintentional. Separation of duties promotes integrity, accountability, and reliability in organizational operations helping to safeguard assets and mitigate risks.

Recommendation 1: The Chief Information Officer should ensure that separation of duty controls reflect NIST guidance and require that all cloud systems have a unique System Owner and AO or AO Designated Representative.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer plans to implement procedures to ensure that separation of duty controls reflect NIST guidance and require that all cloud systems have a unique System Owner and designated AO or AO Designated Representative.

A Cloud System Was in a Production Environment Without Proper Security Documents

We researched TFIMS for the 50 cloud systems and identified one cloud system that is operating in a production environment without a required ATO memorandum and FSTAR document. TFIMS is the authoritative repository for system security documents, and it should contain the system ATO memorandum and the FSTAR document.

According to the IRS Cloud Continuous Monitoring Standard Operating Procedure (SOP), an ATO memorandum resulting from the Cloud Security Assessment and Authorization Methodology process shall be signed by the AO prior to a system's deployment.[4] It is the AO's responsibility to allow or deny the ATO memorandum for systems under their purview in accordance with the organization's risk tolerance throughout the operational life of the system.

In addition, all IRS FISMA-reportable systems are required to be registered in TFIMS in accordance with FISMA, Office of Management and Budget, and NIST requirements. All IRS FISMA systems shall be categorized for impact level, and an individually tailored baseline suite of control requirements shall be established in accordance with NIST or FedRAMP requirements based upon the computing environment.[5] No IRS FISMA systems shall operate in a production environment or process production data without going through an assessment and authorization process and obtaining authorization from an AO. The AOs will make risk management decisions, to include decisions to avoid, accept, or mitigate risk, and shall ensure that those decisions are implemented.[6]

We contacted the business unit that operates the system to obtain further information about the status of the system and its documentation. The business unit indicated the system was a pilot project, and therefore it did not require an approved ATO memorandum. The business unit officials stated that the system is still going through the development process and will not go into production until an estimated six to eight months in the future. While it is accurate that

[4] IRS, *Cybersecurity Cloud Program Management Office Information System Security Officer Cloud Continuous Monitoring Standard Operating Procedures* (Feb. 2023).

[5] NIST, Special Publication 800-53, Rev 5, *Security and Privacy Controls for Information Systems and Organization* (Sept. 2020).

[6] IRS, Internal Revenue Manual 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (Dec. 2023).

a pilot project can operate in a production environment without an ATO memorandum, this system does not meet the requirements for a pilot based on our analysis of the circumstances.

According to IRS guidance, a pilot is a limited version (limited functionality or limited number of users, *etc.*) of the system that is deployed to discover and solve problems before full implementation.[7] This would include technology demonstrations of hardware, software, or both, that are targeted for production systems and tested for a short duration. The system in question has been operating in a production environment for over two years, with additional time expected before it meets all requirements for actual deployment. We determined that this extended time period is not compliant with the requirement that a pilot be of a short duration; and therefore, the system should not still be operating in a production environment without authorization.

Moving a cloud system into a production environment without an official ATO memorandum or proper security documentation could expose the IRS to significant risks such as security breaches, compliance issues, and operational disruption.

Recommendation 2: The Chief Information Officer should ensure that the cloud system immediately completes its pilot program and that an ATO memorandum is approved for the system to remain in production.

> **Management's Response:** The IRS agreed with this recommendation. The Chief, Criminal Investigations Officer, in conjunction with the Chief Information Officer, plans to ensure that the system obtains an ATO memorandum.

The Processes to Maintain Cloud Systems' Security Were Not Effective

We evaluated the security processes of the 50 cloud systems on TFIMS as of November 9, 2023, and identified several issues. The security process includes monthly continuous monitoring executive summary reports (hereafter referred to as summary report). The summary report provides a baseline for the vulnerabilities for each system, their remediation efforts, and the controls that are applicable to each system.

Cloud ISSOs were not preparing summary reports or reports were missing critical elements

Cloud ISSOs were not preparing summary reports as required

The IRS was not preparing summary reports for 11 (22 percent) of 50 cloud systems every month as required. Summary reports for the remaining 39 (78 percent) of 50 cloud systems were prepared as required. The Cloud Continuous Monitoring SOP requires cloud ISSOs to prepare a monthly summary report for each of their assigned systems and provide it to the system's AO.

February 2024 summary reports for five of the 11 cloud systems were not prepared for the following reasons:

- One of the systems is a non-containerized cloud system under contract deliverable.

[7] IRS, *Enterprise Lifecycle Security Guidance (ESG) for Pilots/Tech-Demos* (May 2016).

- One of the cloud systems is the pilot system, noted previously, in a production environment without proper security documents.
- Two of the cloud systems' summary reports are included in contract deliverables and not on the summary report template.
- One of the cloud systems the IRS provided the March 2024 summary report. The IRS reported that the February 2024 summary report was not created because the application was still in their Cloud Annual Security Control Assessment FSTAR phase.

We determined the other six summary reports were not completed by interviewing the cloud ISSOs assigned to the 50 cloud systems (some cloud ISSOs are responsible for multiple systems). Five cloud ISSOs stated they did not prepare the required summary reports across a total of six (12 percent) cloud systems. The summary reports were not prepared and provided to the AO for differing reasons. For example, in one case, the ISSO had been in the position for 12 months and was unaware of the requirement to prepare the summary report. Overall, we determined there was a lack of management oversight ensuring submission of the summary reports.

Management Action: In March 2024, IRS management reported that the ISSOs were preparing February summary reports for the six cloud systems missing the reports, which we were able to verify.

Recommendation 3: The Chief Information Officer should ensure that summary reports are timely created for all cloud systems as required with sufficient oversight by the AOs.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer plans to ensure that summary reports are timely created for all cloud systems as required with sufficient oversight by AOs.

Summary reports were missing a critical element

We reviewed the February 2024 summary reports for 45 of the 50 cloud systems and identified that the reports were missing required information.[8] For the 45 cloud systems reviewed, the number and status of the Plan of Action and Milestones (POA&M) were captured on the summary reports. However, 31 (69 percent) of the 45 cloud systems' summary reports were missing the POA&Ms weakness identification number. Therefore, we were unable to track the POA&Ms in TFIMS. The remaining 14 (31 percent) of the 45 cloud systems reports included the POA&Ms weakness identification number.

The ISSOs must use the summary report template to prepare the report and the template has an element to capture POA&M information. During our review, we identified that some ISSOs included the POA&M weakness identification numbers in the summary report for TFIMS tracking as a best practice. According to the IRS's SOP, each POA&M requires an identification number specific to the weakness.[9] The weakness's identification number provides specific information about the POA&M. We reviewed the Cloud Continuous Monitoring SOP and were unable to find procedures on how to properly complete the POA&M information in the summary reports.

The ISSOs prepare the summary reports and provide them to system AOs so they can evaluate

[8] As previously discussed, five of the cloud systems did not have summary reports for us to test.

[9] *IRS Enterprise Federal Information Security Management Act Plan of Action and Milestones Standard Operating Procedure* (Jan. 2024).

the current security of the systems they are responsible for. When these reports are not created, or lack sufficient information, it increases the risk of the AO overlooking crucial changes or negative developments in system performance and security. This could potentially increase exposure to vulnerabilities and security threats that could lead to the compromise of taxpayer data.

Recommendation 4: The Chief Information Officer should ensure that the Cloud Continuous Monitoring SOP reflect that all summary reports are required to have a unique POA&M identification number when identifying weaknesses.

Management's Response: The IRS disagreed with this recommendation. In accordance with FedRAMP Continuous Monitoring guidance, the Cloud Continuous Monitoring SOP contains procedures for the POA&M information in the summary report to include counts of open POA&Ms and inclusion of the unique ID [identification number] is not essential information to make risk management decisions. The IRS is actively working an open Planned Corrective Action to ensure that the FedRAMP continuous monitoring security review guidelines and report template are updated to include additional report elements to make informed and accurate risk management decisions.

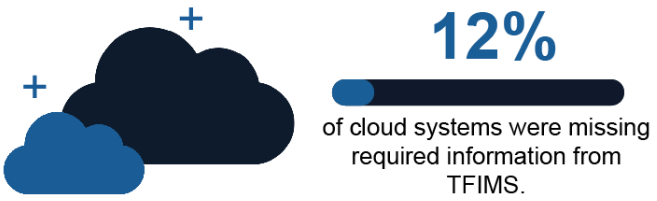
Office of Audit Comment: The IRS cited a Planned Corrective Action in its disagreement that resulted from a prior audit report recommendation where we stated the IRS did not provide summary report elements, such as the name of the preparer and AO, and the date the summary report was prepared, received, and reviewed, to effectively document security reviews.[10] In another audit report, we found that the IRS had 2,555 open POA&Ms.[11] Our current recommendation, if implemented, would address ongoing POA&M documentation issues by standardizing a practice already adopted within 31 percent of the existing summary reports. Our current recommendation would also help AOs to efficiently identify existing system POA&Ms by including a unique identification number within the summary report.

Required ATO memorandum and original ATO date were missing from TFIMS

We analyzed the information available in TFIMS for the 50 cloud systems we identified as of November 9, 2023, to determine if their ATO memorandum approval information was complete and accurate. The approval information for 44 (88 percent) of 50 cloud systems reviewed was complete and accurate in TFIMS. The following 6 cloud systems had items missing from TFIMS:

[10] Treasury Inspector General for Tax Administration, Report No. 2024-200-032, *Actions Have Been Taken to Improve Security Controls for the Planned Expanded Use of Login.gov; However, Additional Security Improvements Are Needed* (July 2024).

[11] Treasury Inspector General for Tax Administration, Report No. 2023-20-042, *Security Weaknesses Are Not Timely Resolved and Effectively Managed* (Aug. 2023).



- Five (10 percent) cloud systems were missing one or more ATO memorandums.
- One (2 percent) cloud system was missing the original ATO memorandum approval date required to be recorded in TFIMS.

The Cybersecurity group is responsible for maintaining this information. The IRS Cloud Security Assessment and Authorization Methodology states that the Cloud Project Management team is responsible for uploading certain information to TFIMS, including the final assessment package, and signed FSTAR, and for updating all relevant fields in TFIMS.[12]

In addition, the Cloud Continuous Monitoring SOP states that the ISSO should ensure that the stakeholder information listed within TFIMS is correct, including the assigned system ISSO information. Through interviews with Cybersecurity officials and the ISSOs and documentation reviews, we determined that the IRS not properly following procedures caused the errors. The lack of essential system documentation and incomplete data fields in TFIMS could make it difficult to verify regulatory compliance of the cloud systems when necessary.

Management Action: As of July 8, 2024, the IRS added the five missing ATO memorandums and updated the ATO memorandum approval date in TFIMS.

Some cloud system documents were missing approvals or were not properly approved

We analyzed the information available in TFIMS for the 50 cloud systems identified as of November 9, 2023, to determine if their ATO memorandums and the FSTAR were properly approved. For the cloud systems reviewed, 46 (92 percent) of 50 ATO memorandums and FSTARs were properly approved. We also identified the following:

- One (2 percent) instance where the FSTAR was signed by the AO after the ATO memorandum approval date, when the ATO memorandum should be approved after the FSTAR.
- Two (4 percent) instances where the AO signed the FSTAR prior to it being completed/signed by the control assessment team that created it.
- One (2 percent) instance where an FSTAR was missing approval signatures from the AO and Cybersecurity executives.

According to the Cloud Security Assessment and Authorization Methodology, the Cloud Security Assessment Report or FSTAR is finalized by the Cybersecurity Cloud Team Lead in preparation for the assessment and authorization exit briefing. The Cybersecurity Cloud Program Manager then routes the signed FSTAR and a draft ATO memorandum to the Security Program Management Office and ISSO to obtain the AO's authorization decision and signature.

We determined that the IRS not properly following procedures caused the errors. According to IRS management, the AO can sign anytime after the Cybersecurity Director's signature. Moving

[12] IRS, *IRS Cloud Security Assessment & Authorization Methodology* (Apr. 2022).

cloud systems into the production environment without a proper ATO memorandum can pose significant risks to the security compliance and operational integrity of systems within the IRS.

Recommendation 5: The Chief Information Officer should ensure that management approvals are consistent and documented per the requirements for cloud systems.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer plans to update the Cloud Assessment SOP to ensure that management approvals are consistent and documented per the requirements for cloud systems.

Security Threat Analysis Reports Were Not Completed for All Cloud Systems

We analyzed the information available in TFIMS for the 50 cloud systems identified as of November 9, 2023, to determine if required FSTARs or equivalent documentation were completed. The FSTAR or equivalent documentation contains a systematic analysis and assessment of a cloud system's security, including which cloud controls failed during the most recent assessment, probable threat characteristics, and the most likely attack vectors. We found that one or more required FSTARs or equivalent documents were not completed for 15 (30 percent) of the 50 cloud systems. The remaining 35 (70 percent) of 50 cloud systems have completed the required FSTARs or equivalent documents.

An FSTAR is required to be completed prior to the initial cloud system ATO memorandum being approved. According to the Cloud Security Assessment and Authorization Methodology, the FSTAR is required annually after authorization as part of continuous monitoring. IRS personnel stated that they did not complete FSTARs because they deferred to the next year after completing the ATO. In addition, IRS personnel substituted a different assessment method, such as a Security Assessment Report, and did not complete the required FSTAR.

The approval of an ATO memorandum without conducting a thorough analysis and assessment of controls undermines the security and integrity of the system, thereby exposing the IRS to various risks and potential harm. Developing an FSTAR for a new cloud system and keeping it updated, helps ensure that the AO, System Owner, and other stakeholders are kept informed of any ongoing issues with specific control weaknesses or other security-related information.

Management Action: As of March 2024, the IRS made the decision to attempt to simplify the naming convention for FSTAR and equivalent documents and replace it with the singular title of Cloud Security Assessment Report. However, as of July 2024, the IRS provided the required FSTAR or equivalent documentation for 14 of the 15 systems. The documentation provided for the remaining system was listed as an interim Cloud Security Assessment Report. For all new cloud systems going through the assessment process, IRS personnel will complete a Cloud Security Assessment Report.

Recommendation 6: The Chief Information Officer should ensure that the Cloud Security Assessment and Authorization Methodology process is completed annually within the FISMA cycle.

> **Management's Response:** The IRS disagreed with this recommendation. The IRS is completing the Cloud Security Assessment and Authorization process annually within the

FISMA cycle in accordance with the IRS Cloud Security Assessment and Authorization Methodology SOP. Additionally, the Treasury Inspector General for Tax Administration acknowledged in the management action within the report that the IRS provided the required FSTAR or equivalent documentation in July 2024.

Office of Audit Comment: Our recommendation would ensure that the annual assessment process is completed approximately every 12 months. Currently, the IRS could complete its FSTARs for two FISMA cycles in as little as two days apart or as much as 23 months apart and still be considered compliant because the FSTAR was completed at some point within each annual FISMA cycle. Federal Agencies are responsible for reporting the effectiveness of agency information security programs on an annual basis. We believe that consistently completing and reporting the results of security assessments and authorizations annually, *i.e.*, every 12 months, is a more effective process for ensuring system security.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to determine whether the FSTARs were prepared and if continuous monitoring efforts were adequate to ensure the security of IRS cloud systems. To accomplish our objective, we:

- Determined the completeness of the IRS's policies and guidance related to the continuous monitoring of cloud systems by comparing the NIST, Cloud Internal Revenue Manual, FedRAMP guidance, and other applicable requirements.
- Identified all the cloud systems in the IRS TFIMS inventory as of November 9, 2023. We then determined if the 50 cloud systems identified in the TFIMS inventory had a completed FSTAR prior to the issuance of the initial ATO by reviewing and comparing the FSTAR and ATO memorandum dates listed in TFIMS.
- Determined if the FSTAR is updated annually as required by evaluating the FedRAMP authorization documentation. We determined if the CSP had prior authorization before being granted an ATO memorandum by the IRS. Determined if all 50 cloud systems identified had FSTAR and an ATO memorandum in TFIMS and if the documents were completed and approved timely.
- Evaluated if actions taken by cloud ISSOs and AOs to monitor and ensure cloud system security were appropriate and consistent by interviewing the ISSOs for the 50 cloud systems regarding their continuous monitoring, ATO, and FSTAR processes. In addition, we reviewed the summary reports for the 50 cloud systems by comparing them to the continuous monitoring templates and the summary reports provided by the IRS.

Performance of This Review

This review was performed with information obtained from the IRS's Information Technology organization located in the New Carrollton Federal Building in Lanham, Maryland, during the period July 2023 through July 2024. 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.

Major contributors to the report were Jena Whitley, Acting Assistant Inspector General for Audit (Security and Information Technology Services); Jason McKnight, Director; Midori Ohno, Audit Manager; Michael Segall, Acting Audit Manager; Joyce Ajanaku, Lead Auditor; Charlene Elliston, Senior Auditor; and Steven Stephens, Senior Auditor.

Data Validation Methodology

During this review we relied on data obtained from the TFIMS system to identify active cloud systems for additional testing. We assessed the reliability of the TFIMS data by performing

electronic testing and reviewing existing information about the data contained in TFIMS. We determined that the data were sufficiently reliable for the purposes of this report.

We determined that TFIMS would be the best data source to meet our audit requirement to identify cloud systems. To accomplish this, we queried the system by two fields, one that denoted whether the system was a cloud system, and another that indicated whether the system was currently in use. We queried TFIMS based on these fields and identified 50 active cloud systems as of November 9, 2023, and downloaded an extract of TFIMS data associated with each of these systems for reference.

The primary use of the TFIMS data was to identify the cloud systems for our review, and we focused our reliability testing on verifying that the number and identities of the cloud systems were complete and accurate. For this purpose, we compared the TFIMS data with another data source, the FISMA Master Inventory. Only minor discrepancies were identified, and this testing provided adequate assurance that the number of cloud systems on TFIMS was sufficiently complete for our audit purpose.

We also performed other testing of the TFIMS data that was downloaded for the 50 systems that were identified. This included reviewing it for missing data, blank fields, duplicate records, values out of range, and invalid dates, no issues were identified. Finally, we researched the TFIMS system, and the controls present to ensure that the data is accurate. Based on established processes and procedures we concluded that sufficient controls were in place to ensure that the data was sufficiently accurate for our purposes.

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 guidance on FedRAMP, the Internal Revenue Manual, the Cloud Continuous Monitoring SOP, and the Cloud Security Assessment and Authorization Methodology. We evaluated these controls by interviewing Information Technology organization personnel, accessing TFIMS information, reviewing available documentation, and analyzing summary reports, ATO memorandums, and FSTARs.

Appendix II

Outcome Measure

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

Type and Value of Outcome Measure:

- Protection of Resources – Actual; 15 cloud systems reviewed did not complete one or more required FSTARs or equivalent documents (see Recommendation 6).

Methodology Used to Measure the Reported Benefit:

We analyzed the information available in TFIMS for the 50 cloud systems we identified as of November 9, 2023, and determined the required FSTARs or equivalent documentation were not completed for 15 of the 50 cloud systems. The FSTAR or equivalent documentation contains a systemic analysis and assessment of a cloud system's security, including which cloud controls failed during the most recent assessment, probable threat characteristics, and the most likely attack vectors. We reported the results to IRS Security Risk Management personnel, who in March 2024 made the decision to simplify the naming convention for FSTAR and equivalent documents and replace it with the singular title of Cloud Security Assessment Report. In July 2024, the IRS provided the required FSTAR or equivalent documentation for 14 of the 15 systems. The documentation provided for the remaining system was listed as an interim Cloud Security Assessment Report.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Rajiv Uppal, Chief Information Officer

Rajiv K. Uppal

Digitally signed by Rajiv K. Uppal
Date: 2024.08.19 08:12:44 -04'00'

SUBJECT: Draft Audit Report – Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes (Audit #2024200003)

Thank you for the opportunity to review and comment on the draft audit report. The IRS appreciates opportunities to improve internal controls and processes related to the security assessment and continuous monitoring of cloud systems.

Over the last two years, the IRS cloud security assessment process has significantly matured utilizing agile principles and risk-based approach to adapt to new cloud requirements and agency priorities. We successfully completed the 2024 annual assessment for Federal Information Security Modernization Act, all while supporting the successful deployments of all Inflation Reduction Act projects. We are committed to continue to improve the IRS security assessment and continuous monitoring processes to make informed risk management decisions. The IRS is committed to the ongoing improvement of cloud security documentation, and we will continue to validate our effectiveness against IRS and Federal Risk and Authorization Management Program security standards.

We agree with recommendations 1, 2, 3, and 5; but disagree with recommendations 4 and 6. Specifically, recommendation 6 has an associated outcome measure related to the protection of resources. As noted in the management action, the IRS provided the evidence to address the outcome. Attached is our corrective action plan which provides more details related to the recommendations from this report.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 317-5000, or a member of your staff may contact Zobaida Sharafeldin, Director, Security Risk Management, at (703) 244-2180.

Attachment

Attachment

Audit# 2024200003, Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes

Recommendations

RECOMMENDATION 1: The Chief Information Officer should ensure that separation of duty controls reflect NIST guidance and require that all cloud systems have a unique System Owner and designated AO or AO Designated Representative.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will implement procedures to ensure that separation of duty controls reflect NIST guidance and require that all cloud systems have a unique System Owner and designated AO or AO Designated Representative.

IMPLEMENTATION DATE: July 15, 2025

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

RECOMMENDATION 2: The Chief Information Officer should ensure that the cloud system immediately completes its pilot program and that an ATO memorandum is approved for the system to remain in production.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief, Criminal Investigations Officer, in conjunction with the Chief Information Officer, will ensure that the system obtains an ATO memorandum.

IMPLEMENTATION DATE: July 15, 2025

RESPONSIBLE OFFICIAL(S): Chief Criminal Investigations (CI)

RECOMMENDATION 3: The Chief Information Officer should ensure that summary reports are timely created for all cloud systems as required with sufficient oversight by AOs.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. The Chief Information Officer will ensure that summary reports are timely created for all cloud systems as required with sufficient oversight by AOs.

IMPLEMENTATION DATE: February 15, 2025

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

Attachment

Audit# 2024200003, Improvements Are Needed in the Cloud Security Assessment, Approval, and Monitoring Processes

RECOMMENDATION 4: The Chief Information Officer should ensure that the Cybersecurity Cloud Program Management Office SOP reflect that all summary reports are required to have a unique POA&M identification number when identifying weaknesses.

CORRECTIVE ACTION 4: The IRS disagrees with this recommendation. In accordance with FedRAMP Continuous Monitoring guidance, the Cloud Continuous Monitoring SOP contains procedures for the POA&M information in the summary report to include counts of open POA&Ms and inclusion of the unique ID is not essential information to make risk management decisions. The IRS is actively working an open Planned Corrective Action (PCA) to ensure that the FedRAMP continuous monitoring security review guidelines and report template are updated to include additional report elements to make informed and accurate risk management decisions.

IMPLEMENTATION DATE: N/A

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

RECOMMENDATION 5: The Chief Information Officer should ensure that management approvals are consistent and documented per the requirements for cloud systems.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The Chief Information Officer will update the Cloud Assessment SOP to ensure that management approvals are consistent and documented per the requirements for cloud systems.

IMPLEMENTATION DATE: July 15, 2025

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

RECOMMENDATION 6: The Chief Information Officer should ensure that the Cloud Security Assessment and Authorization process is completed annually within the FISMA cycle.

CORRECTIVE ACTION 6: The IRS disagrees with this recommendation. The IRS is completing the Cloud Security Assessment and Authorization process annually within the FISMA cycle in accordance with the IRS Cloud Security Assessment & Authorization Methodology standard operating procedures. Additionally, TIGTA acknowledged in the management action within the report that IRS provided the required FSTAR or equivalent documentation in July 2024.

IMPLEMENTATION DATE: N/A

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

Appendix IV

Glossary of Terms

Term	Definition
Annual Security Control Assessment	The annual testing and/or evaluation of a third of management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security.
Authorization-to-Operate	The management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorizing Official	An official 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.
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.
Federal Information Security Modernization Act of 2014 Cycle	A yearly cycle from July 1 to June 30 of the following year.
Federal Risk and Authorization Management Program	A Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Federal Risk and Authorization Management Program Security Threat Analysis Report	Provides the AO with a systematic analysis of which controls failed, given the nature of the system, the probable threat characteristics, and the most likely attack vectors. A threat analysis answers questions like "Where am I most vulnerable for attack?," "What are the most relevant threats?," and "What do I need to do to safeguard against these threats?" thus enabling informed risk management decisions.
Information System Security Officer	An individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or system owner for maintaining the appropriate operational security posture for a system or program.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

Term	Definition
System Owner	The agency official responsible for the overall development, integration, modification, and operation and maintenance of an information system.
Treasury FISMA Inventory Management System	The official FISMA data repository for all Department of the Treasury bureaus. The data maintained in this repository are used as part of the Department of the Treasury's efforts to comply with the E-Government Act of 2002 as well as NIST and Office of Management and Budget regulations and guidance.

Appendix V

Abbreviations

AO	Authorizing Official
ATO	Authorization-to-Operate
CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
FISMA	Federal Information Security Modernization Act of 2014
FSTAR	FedRAMP Security Threat Analysis Report
IRS	Internal Revenue Service
ISSO	Information System Security Officer
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
SOP	Standard Operating Procedure
TFIMS	Treasury FISMA Inventory Management System

To report fraud, waste, or abuse,
contact our hotline on the web at www.tigta.gov or via e-mail at oi.govreports@tigta.treas.gov.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at www.tigta.gov/form/suggestions.

Information you provide is confidential, and you may remain anonymous.