TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements

January 23, 2024

Report Number: 2024-200-009

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

HIGHLIGHTS: Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements

Final Audit Report issued on January 23, 2024 **Report Number 2024-200-009**

Why TIGTA Did This Audit

Cloud computing is a range of services delivered over the Internet. At the IRS, its cloud environment includes managed services consisting of information technology solutions provided by third parties, *i.e.*, managed service providers, via contracts. These cloud managed services contracts (hereafter referred to as cloud services contracts) are the legal and binding agreement between the IRS and the third parties providing the cloud services.

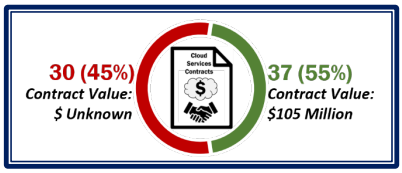
This audit was initiated to assess the IRS's efforts to provide effective management and oversight of cloud services contracts.

Impact on Tax Administration

The Inflation Reduction Act of 2022 provides the IRS $4.8 billion for modernization efforts, including the expansion of cloud migrations. The inability to identify all cloud services contracts and to determine the contract values of cloud applications increases the risk of potential lost cost savings and duplication of cloud services as well as making uninformed financial decisions. When service level agreements (SLA) are inconsistently and ineffectively used, the IRS may be unable to successfully manage risks, ensure that service levels are met, and apply applicable penalties. Further, routinely bypassing the Cloud Front Door process creates confusion and leads to inefficiency for applications migrating to the cloud.

What TIGTA Found

The IRS is unable to locate all cloud services contracts. After searching for nearly three months, the cloud services contracts for 65 (97 percent) of 67 cloud applications on a *Cloud Inventory Report* were located, but the contracts for two (3 percent) applications are missing. As shown in the figure, the IRS is also unable to determine the cloud services contract values.



The IRS is not consistently and effectively using the SLAs. A review of five cloud services contracts determined that four contracts included the SLAs, but one of the contracts containing the SLAs did not include a penalty for not meeting the service level. The remaining cloud services contract did not include any SLAs or penalties as required by applicable standards. Further, applicable contract clauses are not always included in the cloud services contracts. While the IRS included applicable contract clauses in four cloud services contracts, it did not include all appliable contract clauses related to contractor security requirements and training for the remaining contract.

None of the 34 cloud applications that were required to engage the Cloud Front Door process fully completed the necessary steps, including obtaining Cloud Governance Board approval. In addition, the IRS does not have an accurate inventory of cloud applications. A comparison between two cloud application inventory reports identified a total of 29 discrepancies. Finally, continuous monitoring security reviews of cloud applications are not documented.

What TIGTA Recommended

TIGTA made seven recommendations to the Chief Procurement Officer. They include developing a process to track cloud services contracts and to determine the contract values by cloud application; and consistently incorporating the SLAs, penalties, and applicable contract clauses into cloud services contracts. TIGTA also made five recommendations to the Chief Information Officer. They include clarifying in a formal policy that applications migrating to the cloud are required to engage and be processed centrally; ensuring that all applications operating in the cloud have obtained governance board approval; and implementing the new security review guidance for continuous monitoring.

The IRS agreed with all 12 recommendations. The Chief Procurement Officer plans to develop an identification and tracking process for cloud services contracts that includes product and service descriptions and contract values, and update a checklist indicating whether SLAs and contract clauses are required in cloud services contracts. The Chief Information Officer plans to implement a new policy requiring all applications migrating to the cloud to follow the centralized process and obtain governance approval, and implement the new security review guidance for continuous monitoring.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

January 23, 2024

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Matthew A. Weir
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements (Audit # 202320014)

This report presents the results of our review to assess the Internal Revenue Service's (IRS) efforts to provide effective management and oversight of cloud managed services contracts. This review is part of our Fiscal Year 2024 Annual Audit Plan and addresses the major management and performance challenges of *Information Technology Modernization* and *Protection of 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 Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

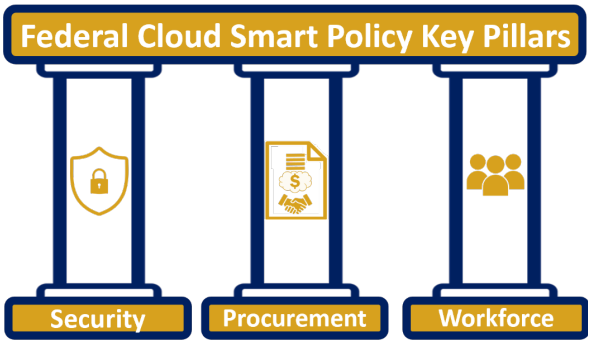
Table of Contents

Appendices

Background

Cloud computing is a range of services delivered over the Internet.[1] At the Internal Revenue Service (IRS), its cloud environment includes managed services consisting of information technology solutions provided by third parties, *i.e.*, managed service providers, via contracts. These cloud managed services contracts (hereafter referred to as cloud services contracts) are the legal and binding agreement between the IRS and the third parties providing the cloud services. Before the IRS awards a contract, the third party's cloud service goes through the IRS's onboarding process, managed by the Information Technology organization's Cloud Management Office (CMO). According to the CMO, its mission is to "deliver a robust and secure ecosystem of cloud-based services and platforms to accelerate IRS modernization programs, increase mission value, and enhance the taxpayer experience." The CMO migrates cloud-based projects, such as applications, to the cloud through its Cloud Front Door (CFD) process. The CFD process serves as the IRS's "on-ramp" to the cloud and is the CMO's centralized processing function for all applications migrating to the cloud. The CMO also manages the Enterprise Cloud Program, a cross-functional program responsible for establishing enterprise-wide cloud capabilities, building the IRS's multicloud system, and providing services to cloud-based projects.

In addition, the CMO directs and coordinates program activities for the IRS's implementation of the Federal Cloud Smart Policy (hereafter referred to as Cloud Smart).[2] Cloud Smart is a multidisciplinary cloud adoption policy for Federal agencies. It requires collaboration between agency leadership, mission owners, technology practitioners, and governance bodies for successful cloud adoptions. The Cloud Smart framework is built on three key pillars: security, procurement, and workforce.



- **Security** – Uses a risk-based approach to secure cloud environments and assures the confidentiality, integrity, and availability of Federal information, whether the information is managed on-premise or off-site by a Government entity or contractor. This includes performing continuous monitoring to detect malicious activity and dedicating efforts to improve system governance.
- **Procurement** – Employs a variety of contracting approaches that leverage the strength of the Federal Government's bulk purchasing power and shared knowledge of sound acquisition principles and relevant risk management practices. The Procurement Pillar includes:

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

[2] The White House, U.S. Chief Information Officer Suzette Kent, *Federal Cloud Computing Strategy* (June 2019). The U.S. Chief Information Officer created Cloud Smart to accelerate agency adoption of cloud-based solutions.

  - **Category Management** – Employs a buy smarter approach, *e.g.*, buy in bulk, to: 1) deliver more savings, value, and efficiency; 2) eliminate unnecessary contract redundancies; and 3) meet Government's small business goals.
  - **Service Level Agreement (SLA)** – Defines the level of performance expected from a service provider, how that performance will be measured, and what enforcement mechanisms will be used to ensure that specified service levels are achieved.
  - **Contract Clause** – Implements the SLAs and ensures that contractors adhere to applicable laws and standard commercial practices.
- **Workforce** – Identifies potential skill gaps that emerge resulting from the transition to cloud-based services and trains staff with the skills and knowledge to keep abreast of new technologies. Training is required and should be addressed in the agency's overall cloud strategy and policies.

The three key pillars must be implemented in unity to achieve cohesion across the agency as it acquires cloud-based services. They are designed to increase return on investments, enhance security, and deliver high-quality services to the American people. In conforming with Cloud Smart, the IRS is accountable for managing the risk of its cloud infrastructure, and that responsibility remains with the IRS even when managed and operated by third parties. This unified approach is essential as the Inflation Reduction Act of 2022 provides the IRS $4.8 billion for modernization efforts, including for the expansion of cloud migrations.[3]

In addition to the CMO, other key stakeholders facilitating the implementation of the IRS's cloud strategy include the Office of the Chief Procurement Officer (OCPO) and the Information Technology organization's Strategic Supplier Management. The OCPO provides procurement services for the entire life cycle of an acquisition, *e.g.*, cloud services contract. According to management from Strategic Supplier Management, it supports the IRS's strategic management of information technology acquisitions and minimizes risk in the acquisition process.

Results of Review

Management and Oversight of Cloud Services Contracts Are Insufficient

The IRS is unable to locate all cloud services contracts

The OCPO identified and provided the cloud services contracts for 24 of 67 cloud applications, but was unable to identify and provide the contracts for the remaining 43 applications listed in the CMO's November 2022 *Cloud Inventory Report* (CIR).[4] We reviewed the OCPO personnel's search methodology and determined that they performed searches of the description fields in the IRS Procurement System and the System for Awards Management for keywords based on the name and type of cloud applications. They also searched for contractor names and other application attributes, *e.g.*, application description. In addition, OCPO personnel stated that they

[3] Public Law No. 117-169, 136 Stat. 1818.

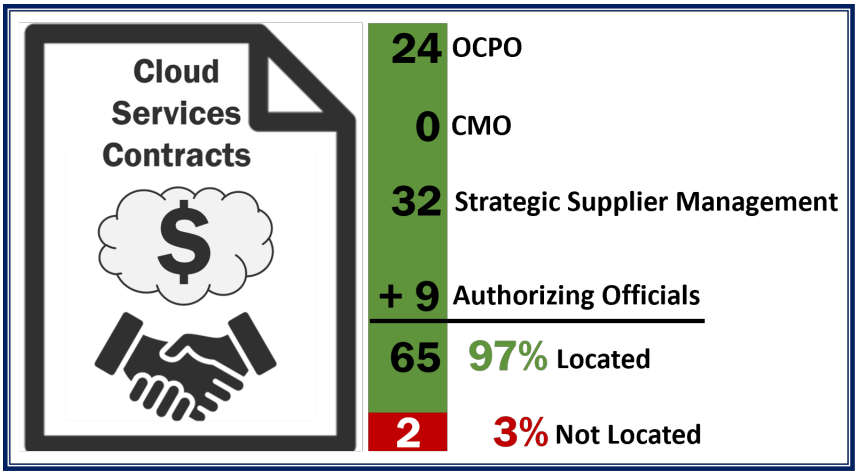
[4] We used the CMO's CIR as our source cloud application inventory list because its CFD process is the central processing function for all applications migrating to the cloud.

used the Product Service Code and the North American Industry and Classification System code in their search to find the cloud services contracts. After researching for nearly two months, at the end of February 2023, OCPO management notified us that they had to stop searching for the remaining cloud services contracts due to resource constraints.[5]

Because the OCPO was unable to find all the cloud services contracts, we requested that the CMO search for the contracts. CMO management stated they were unable to provide any of the cloud services contracts because they do not provide oversight of the contracts. As a result, we requested that Strategic Supplier Management search its records to identify and provide the cloud services contracts. Strategic Supplier Management personnel canvassed cloud application points of contact listed in the IRS As-Built Architecture and were able to provide the cloud services contracts for an additional 32 cloud applications. Finally, we requested that the cloud application Authorizing Officials, who are listed on the CIR, identify and provide the cloud services contracts, and they were able to provide the contracts for another nine applications.

Collectively, the OCPO, Strategic Supplier Management, and the Authorizing Officials identified and provided the cloud services contracts for 65 (97 percent) of 67 cloud applications. After searching for nearly three months, from January through March 2023, the cloud services contracts for the remaining two (3 percent) cloud applications were not found. Figure 1 summarizes the sources that provided the cloud services contracts.

Figure 1: Summary of Cloud Services Contracts Provided by Source



Source: Treasury Inspector General for Tax Administration's analysis and summary of cloud services contracts provided by source.

According to the Government Accountability Office's *Standards for Internal Control in the Federal Government* (Sept. 2014), "Documentation is a necessary part of an effective internal control and is required for the effective design, implementation, and operating effectiveness of an entity's internal control system." *Internal Revenue Service Acquisition Policy, January 2023, FY [Fiscal Year] 2023 Edition, Version 1.0*, states that contracting officers shall store the final and/or approved version of contract documents electronically in the Procurement System's Folders Management module to provide a complete history of the acquisition. It also provides a contract file content checklist that establishes naming conventions and an organizational

[5] OCPO management provided one of 24 cloud services contracts in late October 2023 after testing was completed and while the report was being written.

structure for all contract documents. Cloud Smart requires collaboration between agency leadership, *e.g.*, Chief Procurement Officer and Chief Information Officer, in the areas of security, procurement, and workforce for successful cloud adoptions.

The OCPO does not have a process to track cloud services contracts, and contracting officers did not always store cloud services contracts in the Folders Management module as required. In addition, according to OCPO management, contracting officers are responsible for the coding and categorization of cloud services contracts when written and input into the Procurement System. However, OCPO management also stated that they do not offer such guidance or training to contracting officers to support uniformity when processing cloud services contracts. Rather, they rely on the contracting officers to obtain this knowledge through guidance from other experienced contracting officers or professional training certifications.

As a result, the OCPO must make various and time-consuming queries of the Procurement System to identify the cloud services contracts. For example, OCPO personnel used the keyword "cloud" to search the description field in the Procurement System, but contracting officers had not been provided guidance or training to include that keyword when entering the contract description. In addition, contract code assignment is essential to identify cloud services contracts from the Procurement System, especially when the Product Service Code and the North American Industry and Classification System code are limited to one entry each and are content-based and subjective. OCPO personnel stated that it would be beneficial and more efficient if the Information Technology organization tracked the contract numbers, which are provided at the time of procurement, along with its inventory of cloud applications.

Without a process in place to track cloud services contracts, not ensuring that all cloud services contracts are stored in the Folders Management module, and not providing contract coding and categorization guidance and training, the IRS is unable to identify all cloud services contracts. Not being able to readily identify cloud services contracts increases the risk of potential lost cost savings and duplication of cloud services, and the inefficient use of resources searching for information in response to stakeholder requests.

The Chief Procurement Officer should:

Recommendation 1: In collaboration with IRS leadership, *e.g.*, Chief Information Officer, develop a process to track cloud services contracts to ensure that contracts for cloud applications can be identified readily.

> **Management's Response:** The IRS agreed with this recommendation. Within the Procurement System's data collection limitations, the OCPO and Chief Information Officer will collaborate to develop an identification and tracking process.

Recommendation 2: Ensure that contracting officers store cloud services contracts in the Procurement System's Folders Management module as required.

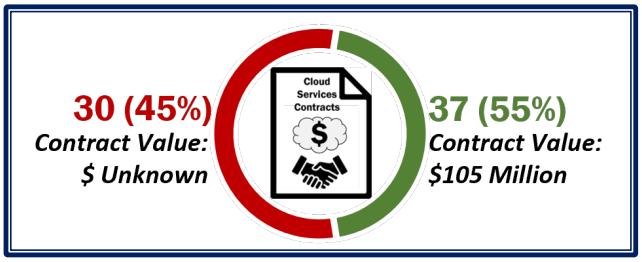
> **Management's Response:** The IRS agreed with this recommendation. The IRS will enhance/update process(es) to confirm that a complete contract file is maintained in the Procurement System's Folders Management module.

Recommendation 3: Develop and provide contract coding and categorization guidance and training to contracting officers.

> **Management's Response:** The IRS agreed with this recommendation. Upon completion of Recommendation 1, the OCPO will disseminate a policy guidance document to all OCPO operational staff related to coding use in the Procurement System. Subsequent training will be provided if deemed necessary.

The IRS is unable to determine the cloud services contract values by cloud applications

Despite locating the cloud services contracts for 65 of 67 cloud applications listed on the CIR, the IRS was able to determine the value of the contracts for only 37 (55 percent) cloud applications of approximately $105 million. The IRS was unable to determine the value of the cloud services contracts for the remaining 30 (45 percent) cloud applications.



Internal Revenue Manual 1.35.24, *Establishing IRS Commitments and Obligations* (Dec. 2019), states that the OCPO is responsible for administering reviews and monitoring and tracking open awards, including contract closeouts or terminations. In addition, suitable documentation is required to be maintained to track contract obligations to ensure that funds are available.

Because cloud services contracts, including contract modifications, may include the purchase of other information technology services and products and the IRS does not have a process to track detailed contract data, specific contract values and obligations associated with each cloud application are not readily identified and determined. The IRS's inability to identify specific cloud services contract values by cloud application increases the risk for making uninformed financial decisions.

Recommendation 4: The Chief Procurement Officer should develop a process to track cloud services contract values by cloud application to ensure that specific contract values and obligations can be readily identified and determined.

> **Management's Response:** The IRS agreed with this recommendation. Using the tracking mechanism from Recommendation 1 and within the Procurement System's data collection limitations, the IRS will maintain an active contract list that will include contract values and the descriptions of products and services (including cloud services).

The SLAs are not consistently and effectively used in cloud services contracts

We selected and reviewed the cloud services contracts for a judgmental sample of five applications from the population of 67 cloud applications listed on the CIR.[6] We determined that each of the cloud services contracts properly contained a signed Authorization to Operate and a completed Form 14775, *Security Compliance Review Checklist for Information Technology Acquisitions*, that was approved by the Information Technology organization's

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

Cybersecurity function. However, we also determined that the SLAs are not consistently and effectively used. Specifically, we found the following:

- Two cloud services contracts included nine SLAs, each with an associated penalty.
- One cloud services contract did not include any SLAs or associated penalties.
- One cloud services contract included an SLA that required the cloud application provide "high availability," defined as having operations available 24 hours a day and seven days a week (99.9 percent of the time). However, the SLA did not specify any performance reporting or monitoring frequency, and there were no associated penalties for not meeting the service level.
- One cloud services contract included seven SLAs, each with an associated penalty for not meeting the service level. One service level was not met in September 2022 and the IRS assessed a penalty. The penalty for not meeting the service level was equal to 3 percent of the monthly cost for the web hosting service, calculated to be $1,017. However, as of May 2023, the IRS had not yet collected the penalty.

In accordance with the *Federal Acquisition Regulation*, performance-based contracts for services shall include measurable performance standards, *e.g.*, in terms of quality, timeliness, and quantity, and the method for assessing contractor performance against those standards.[7] Jointly, the Cybersecurity and Infrastructure Security Agency, the U.S. Digital Service, and the Federal Risk and Authorization Management Program (FedRAMP) issued the *Cloud Security Technical Reference Architecture* (June 2022), which states that agencies should carefully set up the SLAs to define expectations and responsibilities with each of their cloud service providers. In addition, the Chief Information Officers Council and the Chief Acquisition Officers Council published best practices in *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT [Information Technology] as a Service* (Feb. 2012). The publication states that agencies should ensure that performance standards such as response time, resolution/mitigation time, or availability are clearly defined within an SLA. An effective SLA should contain a sufficient penalty so that failure to meet a performance standard creates an undesired business outcome for the service provider.

OCPO management stated that instead of including specific SLAs, they default to their ability to post negative comments about the contractor in the Contractor Performance Assessment Reporting System following each contract period of performance or to terminate the contract entirely for severe deficiencies.

Without the OCPO and the Information Technology organization ensuring that the SLAs for cloud services contracts are consistently and effectively used, the IRS may be unable to successfully manage risks, ensure that service levels are met, and apply applicable penalties.

[7] 48 C.F.R. § 37.601 (2021).

The Chief Procurement Officer should ensure that:

Recommendation 5: Contracting officers consistently and effectively incorporate the SLAs, including penalties for not meeting service levels, into cloud services contracts.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will update the Procurement Acquisition Document Checklist to include a box for the requiring office to indicate whether the requirement will include cloud services. If this box is selected, the OCPO will require that the needed SLAs be included in the acquisition package.

Recommendation 6: The penalty of $1,017 is collected from the managed service provider for not meeting the service level.

> **Management's Response:** The IRS agreed with this recommendation. The IRS already collected the penalty from the managed service provider: $217.63 on June 13, 2023, and the remaining $799.57 on June 23, 2023.

Management Action: In response to this finding, the IRS provided documentation supporting that in June 2023, it collected the $1,017 penalty from the contractor for not meeting the service level.

Applicable contract clauses are not always included in cloud services contracts

Using the same judgmental sample of five cloud applications, we reviewed their respective cloud services contracts and determined that not all contracts included the applicable contract clauses intended to manage security risks for cloud applications. Specifically, the cloud services contracts for all five cloud applications included the mandatory contract clause to prohibit the use of hardware, software, and services developed or provided by a specific contractor and other covered entities. Four of five cloud services contracts included the applicable contract clauses, dependent upon whether purchasing a cloud product or service, from the *IRS Acquisition Policy* (Nov. 2020).[8] However, the remaining cloud services contract for the purchase of cloud services included only three of seven applicable contract clauses related to contractor security requirements and training.

The *Federal Acquisition Regulation* requires that contracting officers ensure that all requirements of law, executive orders, regulations, and all other applicable procedures, *e.g.*, adding applicable contract clauses in cloud services contracts, have been met before entering the contract.[9]

According to OCPO management, the contracting officer omitted the four applicable contract clauses in error. In addition, OCPO management stated that the applicable contract clauses

[8] IRS Acquisition Policy 1052.204-9000, *Submission of Security Forms and Related Materials*; 1052.204-9002, *IRS Specialized Information Technology Security Training (Role-Based)*; 1052.224-9000, *Safeguards Against Unauthorized Disclosure of Sensitive but Unclassified Information*; 1052.224-9001, *Mandatory IRS Security and Privacy Training for Information Systems, Information Protection and Facilities Physical Access*; 1052.239-9007, *Staff-Like Access, Use or Operation of IRS Information Technology Systems*; 1052.239-9008, *Information Systems and Information Security Controls for Contracting Actions Subject to Internal Revenue Manual 10.8.1, Information Technology Security, Policy and Guidance*; and 1052.239-9009, *Information Systems and Information Security Controls for Contracting Actions Subject to Publication 4812, Contractor Security and Privacy Controls*.

[9] 48 C.F.R. § 1.602 (2021).

should have been included and that they would modify the cloud services contract to add the applicable contract clauses. When all applicable contract clauses are not included in cloud services contracts, it exposes the IRS to increased risk.

Recommendation 7: The Chief Procurement Officer should ensure that contracting officers include all applicable contract clauses in cloud services contracts.

> **Management's Response:** The IRS agreed with this recommendation. The IRS will update the Procurement Acquisition Document Checklist to include a box for the requiring office to indicate whether the requirement will include cloud services. The contracting officers will ensure that all applicable security provisions and clauses are included in the solicitations and contracts when this box is selected.

Recommendation 8: The Chief Information Officer should ensure that a modification is executed to the cloud services contract identified as an exception to include contract clauses related to contractor security requirements and training.

> **Management's Response:** The IRS agreed with this recommendation. The OCPO will ensure coordination to verify that identified cloud services contracts contain required contractor security contract clauses and will modify contracts requiring updated security clauses.

Management and Oversight of the Enterprise Cloud Program Are Deficient

None of the applications operating in the cloud completed the required CFD process

The Information Technology organization instructs stakeholders to use the CFD and complete its four-step process for all applications migrating to the cloud. However, we determined that none of the 34 cloud applications listed on the CIR fully completed the CFD process as part of the IRS's Enterprise Cloud Program.[10] Specifically,

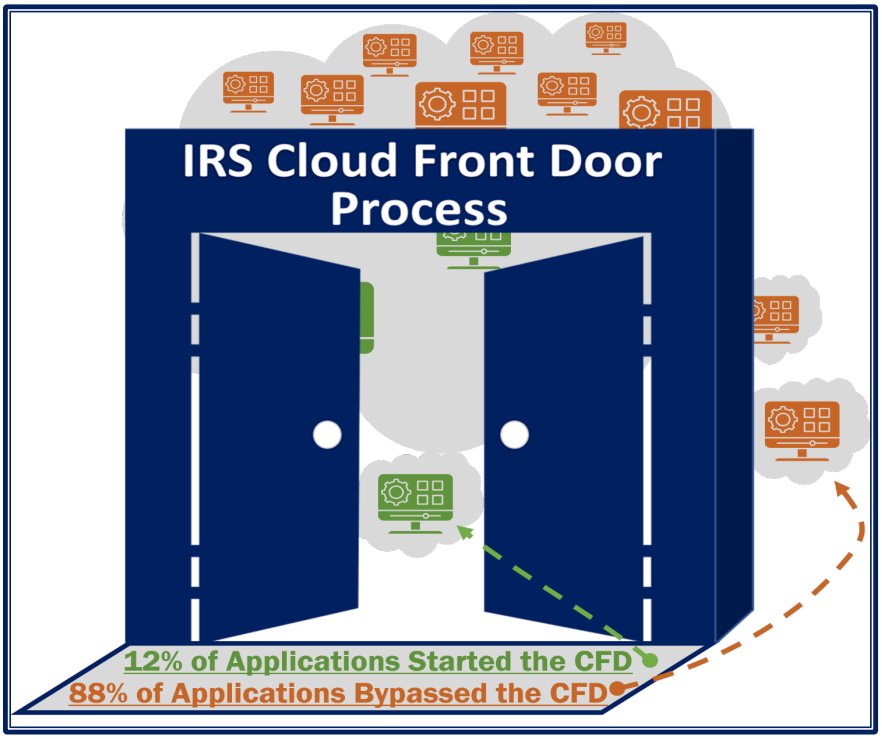
- 30 (88 percent) cloud applications for which the CMO was unable to provide any documentation to support that the applications started the CFD process.
- 4 (12 percent) cloud applications completed some of the CFD four-step sequential process.
  - 4 cloud applications completed Step 1, prepare and submit the cloud intake form.
  - 2 cloud applications completed Step 2, obtain the cloud readiness score.
  - 3 cloud applications completed Step 3, complete the cloud readiness assessment.[11]
  - 0 cloud applications completed Step 4, obtain Cloud Governance Board approval.

[10] Because the CMO was established in February 2020, only 34 of 67 cloud applications on the CIR were required to complete the CFD process.

[11] One cloud application bypassed Step 2 and did not obtain a cloud readiness score.

Figure 2 depicts that most cloud applications bypassed the CFD process.

Figure 2: Most Cloud Applications Bypassed the CFD Process



Source: Treasury Inspector General for Tax Administration's analysis of submitted cloud intake forms for cloud applications on the CIR.

The cloud intake form provides the CMO with initial information about the cloud application to assign a cloud readiness score. The cloud readiness score is used to rank and prioritize cloud applications that provide the most value, in areas of business processes and technical readiness, for migration to the cloud. The CMO then completes a cloud readiness assessment to identify the highest priority applications, and the assessment is sent to the Cybersecurity function for review and approval that the application meets FedRAMP requirements and can be deployed to the cloud. The final step in the CFD process is to obtain Cloud Governance Board approval.

The Taxpayer First Act § 2101, *Management of Internal Revenue Service Information Technology*, states that the IRS Chief Information Officer has centralized responsibility with respect to all development, implementation, and maintenance of information technology for the IRS.[12] Information Technology organization guidance, *Cloud Front Door Process Overview and Backlog Review* (Sept. 2022), states that the CFD process is designed to serve as the IRS's pathway to the cloud and is the CMO's centralized processing function for existing application migrations to the cloud and new tool or service cloud adoptions. The guidance also states that the Cloud Governance Board's review and approval is a required step for an application to operate in the cloud. Cybersecurity function guidance, such as the *Cloud Cybersecurity Authorization Playbook* (Apr. 2022), states that cloud project managers must engage the CFD process to obtain an Authorization to Operate using cloud services. In addition, the CMO's own published guidance,

[12] Pub. L. No. 116-25, 133 Stat. 981 (codified in scattered sections of 26 U.S.C.).

Frequently Asked Questions (Sept. 2022), instructs business units to "Start at the CFD!" when considering using a cloud service.

CMO management stated that there is no formal policy mandating applications engage and be processed through the CFD to operate in the cloud, despite multiple guidance documents stating to the contrary. For example, the CMO's published guidance and website instruct stakeholders to use the CFD process for applications migrating to the cloud. CMO management also stated that a cloud application could obtain governance board approval from either the Cloud Governance Board or the application's own dedicated program/local governance board. To determine whether cloud applications obtained approval from its own dedicated program/local governance board, we reviewed the same judgmental sample of five applications. We determined that three cloud applications obtained and two cloud applications did not obtain approval from their own dedicated program/local governance board (which includes representatives from the Information Technology organization). However, the last step in the CFD process specifies that a cloud application obtain Cloud Governance Board approval, not approval from the application's own dedicated program/local governance board. In March 2023 (during our review), the CMO changed its CFD process so that the Cloud Governance Board is no longer the only governing body responsible for approving applications to operate in the cloud.

The CMO did not provide centralized management and oversight of the Enterprise Cloud Program. As a result, the CFD process is routinely bypassed, creating confusion and leading to inefficiencies for applications migrating to the cloud. For example, Cybersecurity function management explained that a business unit had purchased an application and requested approval to operate it in the cloud. When the Cybersecurity function realized that the application had not completed the CFD process, it denied the request and sent the business unit to the CMO to complete the CFD process. In another example, a business unit started but did not complete the CFD process and requested Cybersecurity function's approval to deploy an application in the cloud. However, the Cybersecurity function was unable to approve the request and notified the CMO that it did "not see any evidence of due diligence or due care from the CMO" in guiding the business unit through the required CFD process.

On August 3, 2023, the Chief Information Officer announced that the CMO was officially phased out and would be transitioning to the Enterprise Cloud Architecture and Design office to better align with the IRS's enterprise goals and modernization efforts. The Enterprise Cloud Architecture and Design office will replace the CMO in all aspects of cloud architecture and design.

The Chief Information Officer should:

Recommendation 9: Clarify in a formal policy that applications migrating to the cloud are required to engage and be processed centrally by the Enterprise Cloud Architecture and Design office.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will implement a new Internal Revenue Manual policy for all applications to follow the centralized process to implement applications in the cloud.

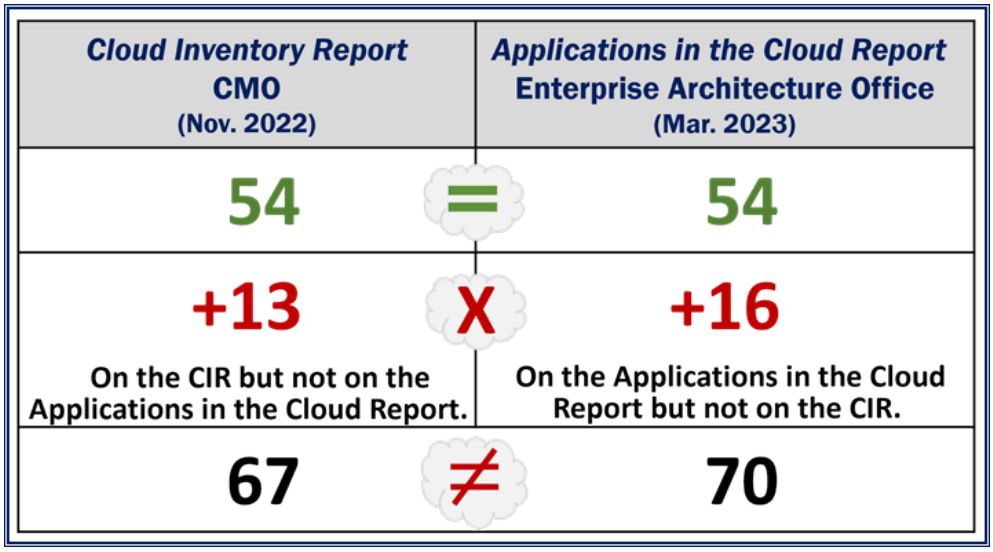
Recommendation 10: Ensure that all applications operating in the cloud have obtained governance board approval.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will ensure that all cloud applications follow the workflow process, which requires governance board approval prior to implementation in the cloud.

The IRS does not have an accurate inventory of cloud applications

The CMO's CIR of 67 cloud applications may be inaccurate. We identified a second cloud application inventory report, *Applications in the Cloud* (Mar. 2023), listing 70 cloud applications from the Information Technology organization's Enterprise Architecture Office.[13] Our review of the two cloud application inventory reports determined that 54 cloud applications were on both reports. However, as shown in Figure 3, we also determined that 13 cloud applications on the CIR were not on the *Applications in the Cloud* report, and 16 cloud applications on the *Applications in the Cloud* report were not on the CIR (a total of 29 discrepancies).

Figure 3: Comparison of Cloud Application Inventory Reports



Source: Treasury Inspector General for Tax Administration's analysis and results from comparing the IRS's CIR and Application in the Cloud Report.

The *Standards for Internal Control in the Federal Government* requires that management process data into quality information that supports the internal control system. Quality information should be appropriate, current, complete, accurate, accessible, and provided on a timely basis. Management uses the quality information to make informed decisions and evaluate the entity's performance in achieving key objectives and addressing risks.

Because the Information Technology organization did not enforce the use of its CFD process, the inventory of cloud applications was inconsistent and inaccurate, and thereby did not meet quality information standards. Without a consistent and accurate inventory of cloud applications, there is an increased risk that the IRS would be unable to maintain internal controls such as FedRAMP continuous monitoring security reviews, maximize benefits by reducing

[13] The *Applications in the Cloud* report listed 72 cloud applications. We determined that two cloud applications were added after the CIR was published and removed them from the *Applications in the Cloud* report.

duplication of cloud services, and ensure that the Chief Information Officer is involved in the acquisition of all cloud applications.

Recommendation 11: The Chief Information Officer should ensure that cloud application inventory reporting is centralized for accuracy.

> **Management's Response:** The IRS agreed with this recommendation. As of July 1, 2023, the As-Built Architecture report replaced the CIR as the definitive source of record for the cloud inventory.

Management Action: In response to this finding, the CMO stopped publishing the CIR in July 2023 and designated the As-Built Architecture as the system of record for the inventory of cloud applications.

FedRAMP continuous monitoring security reviews of cloud applications are not documented

The Cybersecurity function is unable to provide documentation that it completed any Fiscal Year 2022 FedRAMP continuous monitoring security reviews of the 67 cloud applications listed on the CIR. Cybersecurity function management explained that they performed the FedRAMP continuous monitoring security reviews but did not document them.

According to the *Standards for Internal Control in the Federal Government*, "Documentation is a necessary part of an effective internal control and is required for the effective design, implementation, and operating effectiveness of an entity's internal control system." In addition, the *FedRAMP Continuous Monitoring Strategy Guide* (Apr. 2018) provides that each month Authorizing Officials are responsible for monitoring their application's security assessment to ensure that the cloud service provider maintains an appropriate risk posture. This includes tracking the remediation of scan vulnerability findings in the Plan of Action and Milestones.

Cybersecurity function management stated that they did not document their reviews because it was not specifically required by FedRAMP guidance. However, in May 2022, the Cybersecurity function issued the revised *Cloud Continuous Monitoring Standard Operating Procedure* requiring that FedRAMP security reviews of cloud applications be documented. Specifically, it states that FedRAMP security reviews will be performed monthly and documented in the new *IRS Cloud ConMon [Continuous Monitoring] Plan* template. The template will then be uploaded to the Treasury FISMA [Federal Information Security Modernization Act of 2014] Inventory Management System.[14] As of March 2023, after nearly a year since the new guidance was issued, the Cybersecurity function was still working to ensure that the cloud continuous monitoring plan template captures sufficient information to document the continuous monitoring security reviews.

Because the IRS did not document its FedRAMP continuous monitoring security reviews, it is unable to support that the cloud service providers are maintaining an appropriate risk posture of its cloud applications and the IRS's continued authorization of the cloud service providers.

[14] Federal Information Security Modernization Act of 2014, 44 U.S.C. § 3551, et seq. (2018).

Recommendation 12: The Chief Information Officer should ensure that the new guidance to document and maintain FedRAMP continuous monitoring security reviews of cloud applications is implemented.

Management's Response: The IRS agreed with the recommendation. The Chief Information Officer will ensure that the new guidance to document and maintain FedRAMP continuous monitoring security reviews is implemented for all cloud applications.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this audit was to assess the IRS's efforts to provide effective management and oversight of cloud services contracts. To accomplish our objective, we:

- Obtained an understanding of and determined whether processes and procedures are followed to manage and oversee cloud services contracts by reviewing Federal and IRS policies, procedures, and guidance as well as industry best practices, and interviewing OCPO and Information Technology organization personnel.
- Determined whether the OCPO and the Information Technology organization are effectively managing and overseeing cloud services contracts by reviewing a judgmental sample of five contracts from a population of 67 cloud applications listed on the November 2022 CIR.[1] The judgmental sample selected provided a representative sample of the population by type of service model, *i.e.*, infrastructure as a service, platform as a service, and software as a service, and by type of service provider, *e.g.*, managed service provider and cloud service provider.

  Specifically, we reviewed the five cloud services contracts to determine whether the IRS is taking the necessary steps to ensure compliance with contract requirements, security of its applications, and contractor deliverables are being met by examining documentation and interviewing OCPO and Information Technology organization personnel. We selected a judgmental sample because we did not plan to project the results to the population.

Performance of This Review

This review was performed with information obtained from the Cybersecurity and Enterprise Operations functions located at the New Carrollton Federal Building in Lanham, Maryland; the Information Technology organization's CMO located in Farmers Branch, Texas; and the OCPO and Strategic Supplier Management located in Washington, D.C., during the period October 2022 through October 2023. 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 Danny Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services); Louis Lee, Director; Catherine Sykes, Audit Manager; Kanika Kals, Acting Audit Manager; William Varnadore, Lead Auditor; Jason Rosenberg, Senior Auditor; and Allen Henry, Auditor.

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

Data Validation Methodology

During this review, we relied on data extracted from the System for Awards Management, USAspending.gov, and the IRS Procurement System that was provided by programmers from the Treasury Inspector General for Tax Administration's Data Center Warehouse. To assess the reliability of the computer-processed data, we evaluated the data by 1) tracing all cloud services contracts provided by the OCPO, Strategic Supplier Management, and Authorizing Officials to the extract of procurement data; 2) reviewing IRS Procurement System documentation; and 3) interviewing agency officials knowledgeable about the data. We also traced the cloud services contracts for our judgmental sample to the IRS Procurement System to ensure that the contract numbers provided were for the cloud applications listed on the CIR. We determined that the data were sufficiently reliable for purposes of this report.

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: Government Accountability Office's *Standards for Internal Control in the Federal Government*, Federal and various IRS policies and procedures related to the management and oversight of cloud services contracts and contract acquisitions as well as industry best practices. We evaluated these controls by interviewing OCPO and Information Technology organization personnel, reviewing documentation related to the management and oversight of cloud services contracts, and reviewing a sample of cloud services contract files.

Appendix II

Outcome Measures

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

Type and Value of Outcome Measure:

- Protection of Resources – Actual; $1,017 in penalties due the IRS from a managed service provider not meeting a service level (see Recommendation 6).

Methodology Used to Measure the Reported Benefit:

We selected and reviewed the cloud services contracts for a judgmental sample of five applications from the population of 67 cloud applications listed on the CIR.[1] We determined that the SLAs are not consistently and effectively used. Specifically, we found that one service level was not met in September 2022 and the IRS assessed a penalty. The penalty for not meeting the service level was equal to 3 percent of the monthly cost for the web hosting service, calculated to be $1,017.

The IRS provided documentation supporting that in June 2023, it collected the $1,017 penalty from the contractor.

Type and Value of Outcome Measure:

- Reliability of Information – Actual; 29 applications not identified or incorrectly identified as cloud applications (see Recommendation 11).

Methodology Used to Measure the Reported Benefit:

Our review of the CMO's CIR of 67 cloud applications and the Enterprise Architecture Office's *Applications in the Cloud* report of 70 cloud applications determined that 54 applications were on both reports.[2] However, we also determined that 13 cloud applications on the CIR were not on the *Applications in the Cloud* report, and 16 cloud applications on the *Applications in the Cloud* report were not on the CIR (a total of 29 discrepancies).

The CMO stopped publishing the CIR in July 2023 and designated the As-Built Architecture as the system of record for the inventory of cloud applications.

Type and Value of Outcome Measure:

- Reliability of Information – Potential; 67 cloud application continuous monitoring security reviews not documented (see Recommendation 12).

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

[2] The *Applications in the Cloud* report listed 72 cloud applications. We determined that two cloud applications were added after the CIR was published and removed them from the *Applications in the Cloud* report.

Methodology Used to Measure the Reported Benefit:

We requested and the Cybersecurity function was unable to provide documentation that it completed any Fiscal Year 2022 FedRAMP continuous monitoring security reviews of the 67 cloud applications listed on the CIR. Cybersecurity function management explained that they performed the FedRAMP continuous monitoring security reviews but did not document them.

Appendix III

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

12/14/2023

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Acting Chief Information Officer
Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2023.12.14 15:30:09 -05'00'

Todd A. Anthony
Chief Procurement Officer
Digitally signed by Todd A. Anthony
Date: 2023.12.14 10:41:58 -05'00'

SUBJECT: Draft Audit Report – Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements (Audit # 202320014)

Thank you for the opportunity to review and comment on the subject draft report and address the observations with the audit team. The IRS appreciates opportunities to improve internal controls and processes related to the management and oversight of cloud computing contracts. We are committed to adhering to best practices for acquiring information technology (IT) as a service and will make a wide range of improvements noted in the report.

Cloud computing is a major part of IRS operations today, and we expect cloud computing will continue to play an important role in the agency's technology transformation moving forward. The IRS leverages cloud-based technologies and embraces modern technology practices—resulting in major improvements to our legacy systems—but more work remains. The design, procurement, and use of cloud computing services at the IRS involves numerous entities within the agency's procurement and IT functions, each with unique requirements and obligations.

We have already implemented corrective actions to address two of the 12 recommendations, and we generally agree with the audit team's remaining recommendations to improve the management and oversight of cloud managed services contracts, including tracking and properly coding cloud service contracts. We are committed to maintaining the integrity of this process and will update the IRS Procurement Acquisition Document Checklist, in addition to a number of other corrective actions and their associated outcome measures.

The IRS values the continued support and assistance provided by your office. If you have any questions, please contact Christopher Pleffner, Associate Chief Information Officer for Enterprise Services, at (240) 613-6169 and/or the Procurement Audit Liaison Team at procurement.audit.mgt.team@irs.gov.

Attachment

Attachment

TIGTA Audit # 202320014 Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements

Recommendations

RECOMMENDATION 1: The Chief Procurement Officer should, in collaboration with IRS leadership, *e.g.*, Chief Information Officer, develop a process to track cloud services contracts to ensure that contracts for cloud applications can be identified readily.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. Within the procurement system's data collection limitations, the Office of the Chief Procurement Officer (OCPO) and Chief Information Officer will collaborate to develop an identification and tracking process.

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer

RECOMMENDATION 2: Ensure that contracting officers store cloud services contracts in the Procurement System's Folders Management module as required.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The IRS will enhance/update process(es) to confirm that a complete contract file is maintained in the Procurement System's Folders Management module.

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer

RECOMMENDATION 3: Develop and provide contract coding and categorization guidance and training to contracting officers.

CORRECTIVE ACTION 3: The IRS agrees with this recommendation. Upon completion of Recommendation One, the OCPO will disseminate a policy guidance document to all IRS OCPO Operational staff related to coding use in the Procurement System. Subsequent training will be provided if deemed necessary.

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer

Attachment
TIGTA Audit # 202320014

RECOMMENDATION 4: The Chief Procurement Officer should develop a process to track cloud services contract values by cloud application to ensure that specific contract values and obligations can readily identified and determined.

CORRECTIVE ACTION 4: The IRS agrees with this recommendation. Using the tracking mechanism from Recommendation 1 and within the procurement system's data collection limitations, the IRS will maintain an active contract list that will include contract values and the descriptions of products and services (including cloud services).

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer

RECOMMENDATION 5: The Chief Procurement Officer should ensure that Contracting Officers consistently and effectively incorporate the service level agreements (SLAs), including penalties for not meeting service levels, into cloud services contracts.

CORRECTIVE ACTION 5: The IRS agrees with this recommendation. The IRS will update the IRS Procurement Acquisition Document Checklist to include a box for the Requiring Office to indicate whether the requirement will include cloud services, and if this box is selected, then OCPO will require that the needed SLAs be included in the acquisition package.

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer

RECOMMENDATION 6: The Chief Procurement Officer should ensure that the penalty of $1,017 is collected from the managed service provider for not meeting the service level.

CORRECTIVE ACTION 6: The IRS agrees with this recommendation. The IRS already collected the penalty from the managed service provider: $217.63 on June 13, 2023, and the remaining $799.57 on June 23, 2023.

IMPLEMENTATION DATE: Not Applicable

RESPONSIBLE OFFICIAL: Not Applicable

Attachment
TIGTA Audit # 202320014

RECOMMENDATION 7: The Chief Procurement Officer should ensure that COs include all applicable contract clauses in cloud services contracts.

CORRECTIVE ACTION 7: The IRS agrees with this recommendation. The IRS will update the IRS Procurement Acquisition Document Checklist to include a box for the requiring office to indicate whether the requirement will include cloud services. The COs will ensure that all applicable security provisions and clauses are included in the solicitations and contracts when this box is selected.

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer

RECOMMENDATION 8: The Chief Information Officer should ensure that a modification is executed to the cloud services contract identified as an exception to include contract clauses related to contractor security requirements and training.

CORRECTIVE ACTION 8: The IRS agrees with this recommendation. The OCPO will ensure coordination to verify that identified cloud services contracts contain required contractor security contract clauses and will modify contracts requiring updated security clauses.

IMPLEMENTATION DATE: June 15, 2024

RESPONSIBLE OFFICIAL: Office of the Chief Procurement Officer and the Office of Chief Information Officer

RECOMMENDATION 9: The Chief Information Officer should clarify in a formal policy that applications migrating to the cloud are required to engage and be processed centrally by the Enterprise Cloud Architecture and Design office.

CORRECTIVE ACTION 9: The IRS agrees with this recommendation. The Chief Information Officer will implement a new Internal Revenue Manual for all applications to follow the centralized process to implement applications in the Cloud.

IMPLEMENTATION DATE: April 30, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

Attachment
TIGTA Audit # 202320014

RECOMMENDATION 10: The Chief Information Officer should ensure that all applications operating in the cloud have obtained governance board approval.

CORRECTIVE ACTION 10: The IRS agrees with this recommendation. The Chief Information Officer will ensure all Cloud applications follow the workflow process, which requires governance approval prior to implementation in the Cloud.

IMPLEMENTATION DATE: April 30, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

RECOMMENDATION 11: The Chief Information Officer should ensure that cloud application inventory reporting is centralized for accuracy.

CORRECTIVE ACTION 11: The IRS agrees with this recommendation. As of July 1, 2023, the As Built Architecture report replaced the Cloud Inventory Report as the definitive source of record for the Cloud inventory.

IMPLEMENTATION DATE: Not Applicable

RESPONSIBLE OFFICIAL: Not Applicable

RECOMMENDATION 12: The Chief Information Officer should ensure that the new guidance to document and maintain FedRAMP continuous monitoring security reviews of cloud applications is implemented.

CORRECTIVE ACTION 12: The IRS agrees with the recommendation. The Chief Information Officer will ensure that the new guidance to document and maintain FedRAMP continuous monitoring security reviews is implemented for all cloud applications.

IMPLEMENTATION DATE: May 15, 2024

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Appendix IV

Glossary of Terms

Term	Definition
As-Built Architecture	The authoritative source of the IRS's information technology and business environments. It documents the production environment of IRS systems, infrastructure, technology platforms, *etc*.
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	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 Computing	Model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, *e.g.*, network, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud Service Provider	A third-party company offering a cloud-based platform, infrastructure, application, or storage services.
Contractor Performance Assessment Reporting System	Web-based Government system where completed performance evaluations are used as a resource in awarding best value contracts and orders to contractors that consistently provide quality and on-time products and services that conform to contractual requirements. Information collected from contracting officers is used by agency source selection officials and contracting officers from across the Government in making award decisions.
Data Center Warehouse	A Treasury Inspector General for Tax Administration repository of IRS data.
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.
Folders Management Module	A part of the IRS Procurement System that stores contract file documents as the IRS's official system of record.
Governance Board	Exists to ensure that the program goals are achieved and that the program and component projects are delivering within their defined scope, schedule, and budget. In addition, the governance board approves risk response plans and milestone exits and resolves escalated issues.

Term	Definition
Managed Service Provider	A third-party company that remotely manages a specified set of information technology processes, such as security, infrastructure, maintenance, support, *etc.*, for end-user systems.
North American Industry and Classification System	Developed as the standard for use by Federal statistical agencies in classifying business establishments for the collection, analysis, and publication of statistical data related to the business economy of the United States.
Procurement Acquisition Document Checklist	A form listing required documents for acquisitions. The form, along with the required documents, must be attached to the shopping cart of each acquisition. This form is not used when exercising an option or requesting an extension or incremental funding.
Procurement System	A system used by the IRS to track obligations, create solicitations and awards, maintain contractor files, and generate reports. Tax check results should be documented by the contracting officer in this system.
Product Service Code	Describes the different types of products and services being purchased.
Security Compliance Review Checklist for Information Technology Acquisitions	Form used to document compliance of information technology acquisition with Federal law, Department of the Treasury regulations, and IRS policies.
Service Level Agreement	Describes the minimum performance criteria a service provider promises to meet while delivering a service, typically also setting out the remedial action and any penalties that will take effect if performance falls below the promised standard.
System for Awards Management	A U.S. Government website used for registering to do business with the Federal Government and viewing contract data, *etc.*

Appendix V

Abbreviations

CFD	Cloud Front Door
CIR	Cloud Inventory Report
CMO	Cloud Management Office
FedRAMP	Federal Risk and Authorization Management Program
IRS	Internal Revenue Service
OCPO	Office of the Chief Procurement Officer
SLA	Service Level Agreement

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.