TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Cloud-Managed Contracts Were Missing Specific Elements of an Exit Strategy

June 22, 2026

Report Number: 2026-200-028

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

HIGHLIGHTS: Cloud-Managed Contracts Were Missing Specific Elements of an Exit Strategy

Final Audit Report issued on June 22, 2026 **Report Number 2026-200-028**

Why TIGTA Did This Audit

Cloud-computing enables convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services). These resources can be rapidly provisioned and released with minimal management effort or cloud provider interactions. An exit strategy allows the agency to evaluate if the current cloud is still the most suitable platform for its operational needs and to plan a seamless transition to an alternative solution.

We assessed the effectiveness of cloud-computing security controls at protecting sensitive taxpayer data, including corrective actions to address our prior recommendations. We also evaluated the exit strategies between the IRS and its cloud service providers.

Impact on Tax Administration

Critical to the success of a cloud security strategy is the assurance of confidentiality, integrity, and availability of federal information. The IRS could be exposed to significant risks and compliance issues without properly documenting the security assessment results for cloud systems. In addition, when the exit strategy is not specifically included in the cloud-managed contracts, it exposes the agency to an increased risk of legal disputes and financial losses.

What TIGTA Found

Cybersecurity Security Risk Management did not comply with the requirements to document the security control assessment results in the workbook for 23 percent (14 of 61) of the cloud-based systems. The IRS implemented a new tool to track assessment results; however, the 14 cloud-based systems have not been assessed using the new tool. The remaining 47 (77 percent) cloud-based systems were compliant with documenting the assessment results.

Our prior audits have consistently identified deficiencies with the IRS's contract processes. We previously reported that the IRS was unable to locate all cloud service contracts and contract documentation was missing or incomplete. Despite our recommendations and corrective actions taken by the IRS, the deficiencies in the contracts have continued.

We attempted to review the 61 cloud-managed contracts to determine whether the contracts included elements of an exit strategy. However, the IRS could not locate 19 (31 percent) of the contracts. For the 42 cloud-managed contracts we reviewed, we determined that:

- 35 (83 percent) contracts did not fully address elements of an exit strategy.
- 7 (17 percent) contracts did not contain references to an exit strategy.

In addition, we found that 82 percent (36 of 44) of the cloud-managed contracts were missing the required contractor performance evaluation in the Contractor Performance Assessment Reporting System. A missing past performance evaluation can potentially lead the IRS to order supplies or services from a contractor with a poor performance evaluation. Performance evaluations were added for 18 percent (8 of 44) of the cloud-managed contracts.

What TIGTA Recommended

We made two recommendations to the Chief Procurement Officer. They included:

- Updating the process to ensure that the elements of an exit strategy are part of the required document approval process.
- Providing contractor officers' representatives with clear roles and responsibilities to ensure that evaluations are completed and entered timely in the Contractor Performance Assessment Reporting System.

The IRS agreed to both recommendations. However, we determined that the IRS would need other actions to address our second recommendation.

TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

June 22, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Report – Cloud-Managed Contracts Were Missing Specific Elements of an Exit Strategy (Audit No.: 2025200004)

This report presents the results of our review of the effectiveness of cloud-computing security controls at protecting sensitive taxpayer data, including corrective actions to address specific TIGTA recommendations, and to evaluate the exit strategies between the Internal Revenue Service and its cloud service providers. This review is part of our Fiscal Year 2026 Annual Program Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data*.

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

Table of Contents

Background

Cloud-computing is a range of services delivered over the internet.[1] It enables convenient, on-demand network access to a shared pool of configurable computing resources (*e.g.*, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interactions. According to the Federal Cloud Smart Strategy, critical to the success of a cloud security strategy is the assurance of confidentiality, integrity, and availability of federal information, whether it is managed on-premises or off-site by a government entity or contractor.[2]

Cloud security assessments

The Internal Revenue Service's (IRS) guidance states that it is imperative to ensure that information systems are secure, resilient, and aligned with both regulatory and business requirements.[3] A security control assessment package contains key documentation used to evaluate whether an information system should be authorized for production deployment. This package is presented to the Cybersecurity Risk Executive and an authorizing official for review and signature, and includes items such as a(n):

- **Assessment Report.** A document that details the risks and vulnerabilities identified during the security controls assessment for the cloud application or system.
- **Security Assessment Plan.** A document that outlines the process for evaluating a cloud application or system's security measures. It includes applicable laws, regulations, standards, and guidance; scope of controls to be tested; methodology; and test plan.
- **Security Test Case Procedure Workbook (STCPW).** A comprehensive report that documents the results of security testing controls identified in the application or system. Specific aspects of the STCPW include security controls such as:
    - Account Management. Defining access privileges or other attributes by account, type of account, or a combination of both.
    - Audit Record Review, Analysis, and Reporting. Information security and privacy related logging performed by organizations.
    - Cryptographic Key Establishment and Management. A parameter used in conjunction with a cryptographic algorithm that determines its operations.
    - Identification and Authentication. The process of establishing the identity of an entity interacting with a system.
    - Least Privilege. The principle that security architecture is designed so that each entity is granted the minimum system authorization and resources needed to perform its functions.

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

[2] The White House, U.S. Chief Information Officer Suzette Kent, *Federal Cloud Computing Strategy*, (June 2019).

[3] *IRS Cloud Security Control Assessment Assessor's Guide* Version 1.5, (May 2025).

- Protection of Information at Rest. The state of information when it is not in process or in transit and is located on system components.
- Transmission Confidentiality and Integrity. Protecting the confidentiality and integrity of transmitted information applies to internal and external networks as well as any system components that can transmit information, including servers, notebook computers, desktop computers, mobile devices, printers, copiers, scanners, facsimile machines, and radios.
- Vulnerability Monitoring and Scanning. Ensuring that the potential sources of vulnerabilities such as infrastructure components (*e.g.*, switches, routers, guards, sensors), network printers, scanners, and copiers are not overlooked. Alongside vulnerability monitoring, vulnerability scanning is a technique used to identify hosts/host attributes and associated vulnerabilities.

A Cloud Security Assessment Report is produced at the conclusion of an initial assessment, an annual assessment, or an event-driven assessment. The report documents the risk and vulnerability count(s) of the application or system and the cloud service provider. In addition, the report provides the Cybersecurity Risk Executive and authorizing official with an understanding of the risks associated with the cloud application/system.

An exit strategy should be factored into cloud solutions

The IRS's cloud environment includes managed services consisting of information technology solutions provided by third parties (*i.e.*, cloud service providers) via cloud-managed contracts. According to National Institute of Standards and Technology (NIST) guidelines, establishing an exit strategy is an important part of the planning process and should be factored into the requirements analysis.[4]

The benefits of having a cloud exit strategy include:

- **Managing Technology, Operational, and Business Continuity Risks.** An exit strategy allows the agency to evaluate if the current cloud is still the most suitable platform for its operational needs and to plan a seamless transition to an alternative solution, either on-premises or with a different cloud service provider.
- **Achieving Flexibility and Scalability.** A well-thought-out cloud exit strategy will ensure that the agency remains resilient, flexible, and in control of its technology infrastructure and data.
- **The Ability to Comply with Laws and Regulations.** Changes in regulations or legal requirements may necessitate a move to another provider or to an on-premises environment to support the compliance standards required for the organization's industry or geographic region.

Prior reporting identified deficiencies within the IRS's cloud security

Between September 2022 through July 2024, we issued four reports evaluating the IRS's cloud security:

[4] NIST, Special Publication 800-144, *Guidelines on Security and Privacy in Public Cloud Computing* (December 2011).

- September 2022: We reported that key security controls were not implemented before placing taxpayer data in cloud-hosted environments.[5]
- March 2023: We reported that the hybrid cloud system's plan of action and milestones were not timely prepared and contained insufficient documentation. In addition, we found that user accounts were not deactivated or disabled timely and privileged user accounts were not monitored on the hybrid cloud system.[6]
- January 2024: We reported that the IRS's oversight of cloud-managed contracts and Service Level Agreements was insufficient. We also reported that the enterprise cloud program was deficient.[7]
- July 2024: We reported that requirements for the cloud service's continuous monitoring security reviews were not completed timely and/or sent consistently to an authorizing official for review. In addition, we reported that the continuous monitoring reports lacked essential report elements.[8]

For our review of the IRS's planned corrective actions, we relied on supporting documentation in the Joint Audit Management Enterprise System. We also requested additional information to support the closure of these planned corrective actions. Our review of this information confirmed that the IRS implemented all 22 recommendations.

Results of Review

Oversight of Cloud-Managed Contracts Needs Improvement

Assessment results were not always fully documented in the Security Test Case Procedure Workbooks

We found that 23 percent (14 of 61) of the cloud-based systems did not comply with requirements to document the security control assessment results in the STCPW.[9] The remaining 77 percent (47 of 61) of cloud-based systems were compliant with documenting the assessment results. Without properly documenting the security assessment results for cloud-based systems, the IRS could be exposed to significant risks and compliance issues. In addition, the IRS will not be able to provide an accurate view of the organizational security posture.

The former Associate Chief Information Officer, Cybersecurity, issued a memorandum on security and compliance requirements for information technology systems. It stated that the IRS

[5] TIGTA, Report No. 2022-20-052, *Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk* (September 2022).

[6] TIGTA, Report No. 2023-20-018, *The Enterprise Case Management System Did Not Consistently Meet Cloud Security Requirements* (March 2023).

[7] TIGTA, Report No. 2024-200-009, *Management and Oversight of Cloud Managed Services Contracts and the Enterprise Cloud Program Need Improvements* (January 2024).

[8] TIGTA, 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).

[9] According to Cybersecurity, Security Risk Management officials, there were 61 cloud-based systems in the production environment as of December 2024. We used this list as the basis for our review.

is managing a significant increase in programs and projects resulting in an increased reliance on the IRS's security policies to meet the rapidly evolving threat landscape. The memorandum referenced eight security controls to help the IRS manage these threats. We reviewed the STCPW which contains these controls that must be tested as part of the overall cloud security assessment. As previously mentioned, the STCPWs included the results for each control tested and a comprehensive report was provided to the Cybersecurity Risk Executive for review and approval.

According to Security Risk Management (SRM) management officials, the assessors were testing the security controls; however, they were not fully documenting the test results. They also stated that the assessors did not have guidance for documenting observations and evidence. As a result, they were using their own interpretation of IRS policies and NIST guidance. Of the 14 cloud-based systems that did not comply, we found:

- The Account Management controls were not documented for 50 percent (7 of 14) of the cloud-based systems.
- The Identification and Authentication controls and Vulnerability Scanning controls were not documented for five cloud-based systems in each control.
- The remaining controls not documented in the STCPW included:
    - Protection of Information at Rest; and Transmission, Confidentially, and Integrity for three cloud-based systems in each control.
    - Cryptographic Key Establishment and Management for two cloud-based systems in each control.
    - Least Privilege; and Audit Record Review, Analysis and Reporting for one cloud-based system in each control.

Management Action: During our review, the IRS finalized an assessor's guide to ensure that appropriate guidance was provided to properly document security controls in the STCPW. We verified that the assessor's guide was part of the process for conducting cloud security assessments. However, the IRS replaced the STCPW process by migrating to a new tool to track assessment results as of July 1, 2025. The new tool tracks the assessment results and identifies areas of security assessments that have not been documented by the assessors. We subsequently verified that the new tool is operating in the production environment; however, we did not verify that the controls were assessed using the new tool.

Security compliance review checklists are not always being completed prior to purchasing cloud-based systems

We found that Cybersecurity Security Services Management (SSM) is not following its processes to ensure that security compliance review checklists are completed and reviewed before acquiring cloud-based systems. Specifically, the requestor must submit the completed *Security Compliance Review Checklist for Information Technology (IT) Acquisitions* form (hereafter referred to as a compliance checklist) as part of obtaining approval for any information technology acquisition. In addition:

- The compliance checklist and all applicable documentation must be included in the acquisition package submitted to the Procurement Contracting Specialist to show evidence of a security review and compliance approval.

- The compliance checklist requires Cybersecurity SSM personnel to complete a security review within 10 business days of receipt from the requestor.

Further, the IRS's policy states that Procurement Contracting Officers shall store the approved version of contract documents electronically in the procurement system.

The Office of the Chief Procurement Officer (OCPO) provided compliance checklists for 92 percent (56 of 61) of the cloud-based systems; however, it could not locate the compliance checklists for the remaining 5 (8 percent) cloud-based systems. Of the 56 provided compliance checklists, we found that 4 percent (2 of 56) were not timely approved. Approval times took 34 and 36 business days respectively, exceeding the required time frame of 10 business days.

Funding approvals of an information technology acquisition without compliance checklists undermines the security and integrity of the application, thereby exposing the IRS to significant risks and potential harm. Security risks include unauthorized access, inadequate security measures, data leakage, data breach, misconfiguration of systems, *etc*.

Management Action: Cybersecurity SSM management provided a management action plan to enhance resource management, improve communication, and review checklist policies. The action plan states that Cybersecurity SSM management is committed to implementing a digital workflow that will streamline operations, reduce processing times, and improve the archiving repository. In addition, OCPO management stated that they plan to implement a process that focuses on a comprehensive review of shopping cart and acquisition package contents.

A lack of procedures led to deficient exit strategies in cloud-managed contracts

According to NIST guidance, an exit strategy should cover:

- Normal termination of the contract (*i.e.*, expiration of the service agreement).
- Unexpected terminations of the contract (*i.e.*, service provider bankruptcy or poor performance).
- Language to protect the IRS's ability to export all the organization's data in a usable format through a secure, reliable, and efficient means, and in a timely manner.
- Language addressing application dependencies on proprietary programming interfaces, system calls, and database technologies, as well as the recovery of useful metadata that may have accumulated within the cloud environment.

The IRS's internal guidance also notes that special contract language to properly address all potential cloud service provider risks include contract exit conditions and contract termination conditions.

We attempted to review all 61 cloud-managed contracts to determine whether the contract included elements of an exit strategy. However, the IRS could not locate the cloud-managed contracts for the 19 (31 percent) systems in the Procurement for Public Sector system. Our prior audits have consistently identified deficiencies with the IRS's contract process. We previously reported that the IRS was unable to locate all cloud service contracts and the contract documentation was missing or incomplete.[10] Despite our recommendations and corrective

[10] TIGTA, Report No 2024-200-009, *Management and Oversight of Cloud Manages Services Contracts and the Enterprise Cloud Program Needs Improvements* (January 2024) and TIGTA, Report No. 2025-108-052, *Despite Previous Recommendations, Contract Documentation Issues Persist* (September 2025).

actions taken by the IRS, the deficiencies in the contracts have continued. The IRS is scheduled to discontinue using the Procurement of Public Sector system by the end of Calendar Year 2026 and transition to a different system. Therefore, we are not making a recommendation to address the concerns with the missing documentation. However, we may consider this for a future follow-up audit after the IRS's transition to the new procurement system.

Of the 42 cloud-managed contracts we reviewed, the IRS located and found:

- 35 (83 percent) contracts did not include all elements of an exit strategy recommended by NIST guidance. For example, one contract reviewed included language to securely transmit data to the IRS. However, the contract did not have language to address transmitting data in a usable format, through reliable and efficient means, in a timely manner.
- 7 (17 percent) of the contracts did not contain references to an exit strategy.

OCPO management stated that for cloud-based services requirements, the required service level agreements should contain the elements of an exit strategy and be included in the acquisition package. However, current OCPO processes do not ensure that elements of an exit strategy and service level agreements are included in the acquisition package.

When the exit strategy is not specifically included in cloud-managed contracts, it exposes the agency to increased risk of legal disputes and financial losses. Establishing an exit strategy early in the planning stage, and periodically reviewing and updating its contents, can minimize the issues encountered with the termination of a service agreement, and the effort required to transition applications to another cloud-based service provider.

Recommendation 1: The Chief Procurement Officer should update the process to ensure that the elements of an exit strategy are part of the required document approval process.

> **Management's Response:** The IRS agreed with this recommendation and will update the Contract File Content Checklist to ensure that all applicable provisions, clauses, and service level agreements are included in cloud service requirements, addressing exit strategy elements. Additionally, the acquisition checklist (pre-award documentation) includes a statement requiring Contracting Officers to ensure that all applicable security provisions and clauses are incorporated into solicitations and contracts when the "cloud services" option is selected. A policy communication will be released with updates.

Evaluations are missing from the Contractor Performance Assessment Reporting System

Of the 61 contracts, we determined that 28 percent (17 of 61) did not require a Contractor Performance Assessment Reporting System (CPARS) evaluation because the cloud-managed contracts did not meet the simplified acquisition threshold, were not due for annual evaluation, or were a blanket purchase agreement. Of the remaining 44 cloud-managed contracts, we determined that 82 percent (36 of 44) of past performance evaluations were missing from the CPARS. Performance evaluations were added to CPARS for 18 percent (8 of 44) of the cloud-managed contracts.

If past performance evaluations for cloud-based system contractors are not entered into CPARS, the IRS may be unable to provide its executives and stakeholders with critical information on the contractor's past performance. This can potentially lead the IRS to order supplies or services from a contractor with a poor performance evaluation.

The Federal Acquisition Regulation requires agencies to prepare performance evaluations for contractors at least annually, and at the time the work under a contract or order is completed.[11] The IRS's Contractor Officer's Representative Handbook requires the past performance evaluations to be completed and stored in CPARS. These evaluations provide management with current, complete, and accurate information on contractor performance for use during contractor selection. This information supports best value in evaluation and selection decisions to reward proven performers and to motivate contractors to perform.

OCPO management officials noted that many challenges exist for achieving CPARS compliance, such as a lack of clear leadership and management oversight. OCPO officials stated that management must communicate compliance as a priority, and managers must facilitate engagement by providing resources and demonstrating support with communication.

Recommendation 2: The Chief Procurement Officer should provide contractor officers' representatives with clear roles and responsibilities to ensure that evaluations are completed and entered annually in the CPARS as required by the Federal Acquisition Regulation.

Management's Response: The IRS agreed with this recommendation and stated it provides at least one CPARS training annually to ensure that contractor officers' representatives understand their roles and responsibilities for completing and entering annual evaluations in CPARS.

Office of Audit Comment: While the IRS agreed with this recommendation, the proposed corrective action does not fully address our concern. The IRS implemented CPARS training several years ago, yet we continue to find that evaluations were not completed as required. Though training may help clarify roles and responsibilities, we believe additional actions are needed to ensure that evaluations are completed and entered into the CPARS as required. For example, as noted in our report, OCPO officials indicated that management needs to communicate compliance as a priority and provide contracting officer representatives with resources and support.

[11] 48 C.F.R. § 42.1502 (2025).

Appendix I

Detailed Objectives, Scope, and Methodology

The objectives of this audit were to determine the effectiveness of cloud-computing security controls at protecting sensitive taxpayer data, including corrective actions to address specific TIGTA recommendations, and to evaluate the exit strategies between the IRS and its cloud service providers. To accomplish our objectives, we:

- Obtained a list of 61 cloud-based systems from Cybersecurity SRM as of December 2024. Cybersecurity SRM exported the list from the Assessment, Authorization, and Risk Governance repository.
- Determined whether the security requirements are assessed and properly documented by obtaining and reviewing security documents (Security Assessment Plan, STCPW, and Cloud Security Assessment Report) to support the population of 61 cloud-based systems. Specifically, we reviewed the NIST guideline controls and traced the security requirements to the Security Assessment Plan, then to the STCPW, and lastly to the Cloud Security Assessment Report.
- Determined whether Cybersecurity SSM management approved information technology acquisitions by obtaining and reviewing compliance checklists to support the approval for purchasing 61 cloud-based services.
- Determined whether the 61 cloud-based systems contained elements of an exit strategy as outlined in the NIST Special Publication 800-144 by obtaining and reviewing cloud-managed contracts.
- Determined whether the Procurement Contracting Officers completed CPARS by obtaining and verifying that the CPARS evaluations were completed and entered in CPARS for the 61 cloud-based systems.

Performance of This Review

This review was performed with information obtained from the Information Technology organization located in the New Carrollton Federal Building in Lanham, Maryland, and the OCPO located in Washington, D.C, during the period August 2024 through October 2025. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Data Validation Methodology

We performed tests to assess the reliability of the data obtained from the Assessment, Authorization, and Risk Governance repository. We evaluated the data by (1) interviewing IRS management knowledgeable about the data; (2) reviewing required data elements; and (3) reviewing the data to detect obvious errors, duplicated values, and unexpected missing data. We

determined that data from the Assessment, Authorization, and Risk Governance repository 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 objectives: NIST guidelines, federal guidance on Federal Acquisition Regulation, IRS policies, *Cloud Security Control Assessments Standard Operating Procedures (SOP)*, and the *IRS Cloud Security Control Assessment Assessor's Guide*. We evaluated these controls by interviewing IRS subject matter experts, comparing relevant inventory data, reviewing available documentation, reviewing management and oversight of cloud-managed contracts, and reviewing system security documents.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

May 12, 2026

MEMORANDUM FOR DIANA M. TENGESDAL
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kaschit Pandya
Chief Information Officer
Kaschit D. Pandya
Digitally signed by Kaschit D. Pandya
Date: 2026.05.12 11:16:39 -04'00'

SUBJECT: Draft Audit Report – Cloud-managed Contracts Were Missing Specific Elements of an Exit Strategy (Audit #2025200004)

Thank you for the opportunity to review and comment on the draft audit report and address your observations with the audit team. The IRS has taken and will continue to take steps to strengthen its cloud management process and remains committed to continuous improvement consistent with established policies and guidelines.

Management agrees with the two recommendations provided by the Treasury Inspector General for Tax Administration. The IRS is committed to fully implementing and documenting all agreed-upon corrective actions. Please refer to the attachment for specific details.

The IRS values the continued support and partnership provided by your office. If you have any questions, please contact me at (202) 315-5000, or a member of your staff may contact Robert King, Coordinating Director, Data & Platform Engineering, at (469) 801-1202.

Attachment

Attachment

Audit #2025200004, *Cloud-managed Contracts Were Missing Specific Elements of an Exit Strategy*

Recommendations

RECOMMENDATION 1: The Chief Procurement Officer should update the process to ensure that the elements of an exit strategy are part of the required document approval process.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Procurement Officer will update the Contract File Content Checklist to ensure that all applicable provisions, clauses, and service level agreements (SLAs) are included in cloud service requirements, addressing exit strategy elements. Additionally, the acquisition checklist (pre-award documentation) includes a statement requiring Contracting Officers (COs) to ensure that all applicable security provisions and clauses are incorporated into solicitations and contracts when the "cloud services" option is selected. A policy communication will be released with updates.

IMPLEMENTATION DATE: December 1, 2026

RESPONSIBLE OFFICIAL(S): Chief Procurement Officer

RECOMMENDATION 2: The Chief Procurement Officer should provide contractor officer's representatives with clear roles and responsibilities to ensure that evaluations are completed and entered annually in the CPARS as required by the Federal Acquisition Regulation.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Procurement Officer provides at least one CPARS training annually to ensure that CORs understand their roles and responsibilities for completing and entering annual evaluations in CPARS.

IMPLEMENTATION DATE: May 15, 2026

RESPONSIBLE OFFICIAL(S): Chief Procurement Officer

Appendix III

Glossary of Terms

Term	Definition
Acquisition Package	Illustrates the product/services that are needed to meet the IRS's missions and goals.
Assessment, Authorization, and Risk Governance	The official Federal Information Security Modernization Act of 2014 document repository of IRS information systems and data mandated by the Department of the Treasury.[12]
Cloud-Computing	A 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 interactions.
Cloud Security Assessment Report	Documents the risk and vulnerability count(s) of the application or system and the cloud service provider/cloud service offering, giving the Cybersecurity Chief Risk Officer and the authorizing official an understanding of the risks associated with the cloud application/system, and cloud service provider and cloud service offering.
Cloud Service Provider	A third-party company that offers a cloud-based platform, infrastructure, application, or storage services.
Contractor Performance Assessment Reporting System	A governmentwide evaluation reporting tool for all past performance reports on contracts and orders.
Cryptographic Algorithm	A well-defined computational procedure that takes variable inputs, often including a cryptographic key, and produces an output.
Federal Acquisition Regulation	The primary acquisition regulation for use by all federal executive agencies in their acquisition of supplies and services with appropriated funds.
Federal Information Security Modernization Act	Focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses.
Information Technology Acquisition	Procurement of an information technology product/service that includes cloud services.
Joint Audit Management Enterprise System	The Department of the Treasury system used by all bureaus to track, monitor, and report the status of internal control audit results. The system tracks specific information on issues, findings, recommendations, and planned corrective actions for the audit reports issued by oversight agencies, such as TIGTA.
Planned Corrective Action	The process to address IRS material weakness, significant deficiencies, and existing reportable conditions through remediation and action plans.

[12] Pub. L. 113-283, 128 Stat. 3073.

Term	Definition
Security Assessment Plan	A document that outlines the process for evaluating a cloud application or system's security measures. It includes but is not limited to the following: applicable law, regulations, standards, and guidance; scope of controls to be tested; methodology, and test plan.
Security Compliance Review Checklist for Information Technology Acquisitions	A 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.
Shopping Cart	Used to request external goods and services and to secure the necessary approval and funding for those goods and services before the request is submitted.

Appendix IV

Abbreviations

CPARS	Contractor Performance Assessment Reporting System
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OCPO	Office of Chief Procurement Officer
SRM	Security Risk Management
SSM	Security Services Management
STCPW	Security Test Case Procedure Workbook
TIGTA	Treasury Inspector General for Tax Administration

To report fraud, waste, or abuse,
contact our hotline on the web at
https://www.tigta.gov/reportcrime-misconduct.

To make suggestions to improve IRS policies, processes, or systems affecting taxpayers, contact us at
TIGTACommunications@tigta.treas.gov.

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