TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The IRS Has Made Limited Progress Implementing Zero Trust Data Principles

March 25, 2026

Report Number: 2026-208-013

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

HIGHLIGHTS: The IRS Has Made Limited Progress Implementing Zero Trust Data Principles

Final Audit Report issued on March 25, 2026 **Report Number 2026-208-013**

Why TIGTA Did This Audit

A data governance strategy outlines how an organization will manage, protect, and use its data assets to achieve its business goals. It is a framework that defines policies, processes, and accountabilities for data, ensuring its quality, security, and accessibility. Essentially, it is the blueprint for how data are managed throughout its lifecycle, from creation to disposal. The Zero Trust Architecture is an end-to-end approach focused on resource protection and the premise that trust is never granted implicitly and must be continually evaluated.

We assessed the IRS's data governance strategy and determined if the agency effectively implemented key controls, processes, and planned deliverables for the Zero Trust Maturity Model Data Pillar's functions.

Impact on Tax Administration

In the current threat environment, the federal government can no longer depend on conventional processes to protect critical systems and data. The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. For tax administration, this means that anything attempting to establish access must be continually verified. This includes each user, application, and transaction.

What TIGTA Found

We agree with the IRS's self-assessment that most of its data pillar maturity ratings are in either the Traditional or Initial maturity stage, meaning that most of its solutions and responses are manual or are in the process of becoming automated. We also found that the IRS has made little progress implementing the Zero Trust Data Pillar functions.

The IRS is in the first stages of development for its Data Inventory Management and Categorization. The IRS developed the Enterprise Data Platform for its data inventory and has onboarded 41 (22 percent) of the 187 data repositories as of October 2025. The IRS has deployed two commercial software solutions for data categorization. However, the IRS has not implemented automated categorization of data due to challenges establishing related policies.

The IRS encrypts data in transit between its locations, and we confirmed that encryption configuration settings are enabled for data transmitted between IRS locations. However, management personnel from the IRS Enterprise Operations function stated that they cancelled plans to encrypt any more systems past June 2025 due to changing priorities at the Department of the Treasury.

In addition, we found that the IRS did not follow its internal policies to ensure the security of encryption keys. Specifically, the combinations for the cabinet locks that contain access cards necessary to log on to the encryption servers were not changed as required and our auditors were allowed to enter limited access areas without signing the appropriate log.

Furthermore, we found that the majority of the IRS data were backed up. However, the IRS does not resolve the requests for data restoration within the required time frames. By not restoring the data in a timely manner, it could impact the ability of the IRS to conduct its business operations.

Finally, the IRS did not meet the requirements to create an Information Resources Management Strategic plan as required by the Office of Management and Budget. The IRS presented different documents as its strategic plan. Our review of these documents found that they did not contain elements such as including the governance boards in these documents.

What TIGTA Recommended

We recommended that the Chief Information Officer evaluate the current data restoration process and streamline processes to ensure that recovery timelines are met and develop a single document to serve as its Information Resources Management Strategic Plan and ensure that the plan includes all required components.

The IRS agreed to both recommendations.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

March 25, 2026

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Diana M. Tengesdal
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The IRS Has Made Limited Progress Implementing Zero Trust Data Principles (Audit No.: 2025208013)

This report represents the results of our review of the Internal Revenue Service's (IRS) data governance strategy and to determine if the IRS effectively implemented key controls, processes, and planned deliverables related to the Zero Trust Maturity Model Data Pillar Functions. This review was part of our Fiscal Year 2025 Annual Audit Plan and addresses the major management and performance challenge of *Protecting Taxpayer Data.*

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

Table of Contents

Background

A data governance strategy outlines how an organization will manage, protect, and use its data assets to achieve its business goals. It is a framework that defines policies, processes, and accountabilities for data; ensuring its quality, security, and accessibility. Essentially, it is the blueprint for how data are managed throughout its lifecycle, from creation to disposal.

In the current threat environment, the federal government can no longer depend on conventional processes to protect critical systems and data. The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted.[1] For tax administration, this means that anything attempting to establish access must be continually verified. This includes each user, application, and transaction.

In August 2020, the National Institute of Standards and Technology (NIST) issued Zero Trust Architecture (ZTA) guidance that provided direction for federal agencies to migrate and deploy ZTA security concepts to an enterprise environment.[2] ZTA is an end-to-end approach to enterprise resource and data security that is focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated.

The purpose of ZTA is to protect sensitive data assets and secure data throughout its lifecycle. The different data pillar functions can be broken down into three stages of data security:

1. **Defining the Data.** This involves creating a data asset inventory, defining the sensitivity and criticality of data, and categorizing the data assets so the appropriate security controls can be applied.
2. **Securing the Data.** The philosophy of zero trust extends to identity and access management that plays a pivotal role in ensuring the confidentiality, integrity, and availability of data within federal systems. In addition, implementing appropriate data security monitoring and controls, such as encryption, is a key element of zero trust data security.
3. **Managing the Data.** This includes the development and enforcement of policies, processes, and controls to protect data from unauthorized access, alteration, or loss throughout its lifecycle. In addition, managing the data involves securing backups and ensuring that data can be recovered within established time frames.

Zero Trust Data Pillar and data security

The Zero Trust Data Pillar outlines a strategic approach to data security, designed to protect and manage all structured and unstructured data within federal systems. It focuses on securing and enforcing access to data at rest and in transit through various methods, including encryption, labeling, data loss prevention strategies, and application of data rights management tools. Additionally, securing data so it is accessed exclusively by authorized users is a primary responsibility of the data pillar.

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

[2] NIST, Special Publication 800-207, *Zero Trust Architecture* (August 2020).

The data pillar is composed of several key functions that are essential for the protection and management of data within ZTA.

- **Data Inventory Management**. Inventorying data allows organizations to efficiently find, access, and use data assets. Policy and program managers not only need to know what data the organization collects and maintains, but also how it aligns with its intended purpose, what condition it is in, and how it is stored and accessed.
- **Data Categorization**. Classifying and labeling data to determine its sensitivity and the security controls needed is the first step. This function is crucial for applying zero trust principles effectively.
- **Data Availability**. Maintaining the integrity and availability of data, even amidst cyber threats, is also a key function. This ensures that authorized users can access data when needed.
- **Data Access**. Controlling and monitoring data access is imperative. By implementing least privilege access controls, only necessary data are accessible to users and systems based on their roles.
- **Data Encryption**. Encrypting sensitive data in transit and at rest with Federal Information Processing Standards validated algorithms protect sensitive data from unauthorized interception or access.
- **Visibility and Analytics Capability**. Continuous monitoring and auditing of data access and usage helps detect and respond to security incidents. This includes maintaining logs and analyzing data access patterns.
- **Automation and Orchestration Capability**. Automating tools and processes streamline security operations and responses.
- **Governance Capability**. Establishing and updating policies and procedures and providing oversight ensures adherence to security standards and practices.

In January 2022, the Office of Management and Budget (OMB) issued a memorandum that described strategic goals that align with the Zero Trust Maturity Model developed by the Cybersecurity and Infrastructure Security Agency.[3] The OMB required agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year 2024. This included completing three tasks related to the data pillar function.

1. Agencies must implement initial automation of data categorization and security responses, focusing on labeling and managing access to sensitive documents.
2. Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.
3. Agencies must work with the Cybersecurity and Infrastructure Security Agency to implement comprehensive logging and information sharing capabilities, as described in OMB August 2021 memorandum.[4] In October 2023, we reported that the IRS did not

[3] OMB, Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (January 2022).

[4] OMB, Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 2021).

meet the required OMB time frames for event logging maturity.[5] In July 2024, the IRS reported that it met event logging maturity levels 1 and 2 requirements and has ongoing efforts to move to event logging maturity level 3 across the organization.

IRS self-assessment of its data pillar maturity rating

There are four stages of maturity defined for each function: Traditional, Initial, Advanced, and Optimal. Traditional is the starting point consisting of manual solutions and responses and security policies that are static instead of dynamic. The maturity rating advances from Traditional to Initial, Advanced and Optimal. Each subsequent stage requires greater levels of protection, detail, and complexity for adoption, *i.e.*, the automation of zero trust functions and processes. Although the Cybersecurity and Infrastructure Security Agency and the OMB did not provide time frames for agencies to advance to a specific stage of maturity, the ultimate goal is to reach the Optimal rating.

The IRS rated its Data Pillar Maturity Rating at the Traditional stages for five of eight key functions necessary to meet its data security and governance goals. We evaluated the status of the IRS's Data Inventory Management, Data Categorization, Governance Capability, Data Availability, and Data Encryption during this review and agree with the IRS's self-assessment. The results of our review are detailed below. We determined that complexity of the remaining functions would require separate audit reviews. Figure 1 shows the IRS's assessment of its maturity rating for the five functions.

Figure 1: IRS's Assessment of its Zero Trust Maturity Ratings for the Data Pillar

Pillar	Function	IRS Maturity Rating	Reviewed by TIGTA
Data	Data Inventory Management	Traditional	Yes
	Data Categorization	Traditional	
	Governance Capability	Traditional	
	Data Availability	Initial	
	Data Encryption	Initial	
	Automation and Orchestration	Traditional	No
	Data Access	Traditional	
	Visibility and Analytics Capability	Initial	

Source: Analysis of IRS maturity ratings.

[5] TIGTA, Report No. 2024-200-005, *The IRS Has Improved Audit Trail Collection; However, Not All Audit Trail Data Are Being Collected and User Account Controls Need Improvement* (October 2023).

Results of Review

There Has Been Little Progress Made Implementing the Data Pillar of the Zero Trust Architecture

During our review, we found that limited progress has been made within two specific functions of the Data Pillar: Data Inventory Management and Data Categorization. As previously noted, the OMB required agencies to implement automation of data categorization and security responses, focusing on labeling and managing access to sensitive documents. However, both the IRS's Data Inventory Management and Data Categorization are at the first stage of development (Traditional).

Data Inventory Management. The IRS is at the Traditional level for Data Inventory Management, *i.e.*, the IRS identified and inventoried some data. To advance to the Initial level of the Zero Trust Maturity Model, the IRS must automate data inventory processes for both on-premise and in cloud environments, covering most agency data, and begin to incorporate protections against data loss.

The IRS developed the Enterprise Data Platform (EDP) as its Data Inventory Management platform. The EDP ingests data from IRS legacy systems and provides IRS personnel access to high quality usable data and analytics in an open platform architecture. According to the EDP project documentation, it will provide users with immediate access to up-to-date, authoritative data to allow IRS employees to be more responsive to evolving customer needs, leading to improved tax compliance. The IRS started onboarding data into the EDP in April 2022. As of October 2025, the IRS has onboarded 41 (22 percent) of 187 data repositories into the EDP.[6]

We have a separate review of the EDP to evaluate the data quality and accuracy, compliance with regulatory requirements and policies, and data security controls to protect sensitive information. We plan to issue this report during Fiscal Year 2026.

Data Categorization. The IRS is at the Traditional level for Data Categorization, *i.e.*, the IRS has limited and *ad hoc* data categorization capabilities. To advance to the Initial level of the Zero Trust Maturity Model, the agency must begin to implement a data categorization strategy with defined labels and manual enforcement mechanisms, *i.e.*, employees manually reviewing data labels are accurate in the absence of an automated tool or process.

The IRS purchased and has deployed two commercial software solutions for data categorization. One solution categorizes files, emails, and internal IRS sites, *e.g.*, SharePoint sites. However, this solution has limited functionality and can only categorize data within one of the IRS's software products. In addition, the data cannot be categorized within some existing IRS systems and there is limited control over who can access the categorized data. The second solution has the capability to scan and categorize data. However, it requires employees to import this data into the EDP.

While both solutions are capable of automated categorization of data, the IRS has not implemented the functionality due to challenges establishing policies for data categorization.

[6] The IRS's As-Built Architecture shows the IRS has 187 data stores as of October 2025. Data stores are added into the EDP based on the IRS's priorities. IRS programs decide when and which data stores need to be onboarded to the EDP.

The IRS does not have a definitive date for when automated categorizing of data will begin. According to personnel from the IRS's Privacy, Governmental Liaison, and Disclosure function, automated data categorization is not being used for the two solutions because federal data standards guidance is not available.

Data Encryption is at the Initial level and plans to encrypt future systems were cancelled

In May 2021, Executive Order 14028, *Improving the Nation's Cybersecurity*, directed agencies to use encryption to protect data at rest, *e.g.*, when it is stored. In addition, OMB Memorandum M-21-31 requires agencies to audit access to any data encrypted at rest in commercial cloud infrastructure, *i.e.*, create an audit log that documents attempts to access the data at rest in the cloud.

During our review, we found that the IRS is at the Initial level for Data Encryption, *i.e.*, the IRS encrypts data in transit and data at rest, when feasible, and it is beginning to formalize management policies and secure encryption keys. To progress to the Advanced level of the Zero Trust Maturity Model, the agency must, for example, encrypt all data at rest and in transit across the enterprise to the maximum extent possible and protect encryption keys.

The IRS encrypts data in transit between its locations. We confirmed that encryption configuration settings are enabled for data transmitted between IRS locations. In addition, the IRS completed encrypting 149 critical systems in December 2023.[7] We reviewed a statistically valid random sample of 50 (34 percent) of the 149 critical systems to verify the encryption status, including 13 High Value Assets managed by the IRS.[8] Seven (14 percent) of the 50 systems in our sample were cloud systems. Although the IRS is not responsible for encrypting the data in the cloud systems, it is required to monitor attempted accesses. For the systems we reviewed, we did not identify any issues.

The IRS had a two-phased approach to implement encryption for its other systems. The first phase covered 291 systems that are classified as Tier I and Tier II systems. As of April 2025, the IRS encrypted 254 (87 percent) of the 291 systems. However, personnel from the IRS's Enterprise Operations function stated that they cancelled plans to encrypt any more systems past June 2025 due to changing priorities at the Department of the Treasury. As a result, the remaining 37 (13 percent) Tier I and Tier II systems in the first phase were not encrypted. In addition, 89 Tier I and Tier II systems from the second phase were not encrypted.

Without encrypting data residing in critical systems, there is a risk of improper access and potential for unauthorized exfiltration of the data, reducing ZTA's ability to enforce encryption and improve data security. In November 2025, personnel from Enterprise Operations informed us that they are planning to resume encryption in Fiscal Year 2026. The risk of improper access and potential data loss will continue to be an area of concern until these plans are approved and implemented.

[7] This included all systems listed in the Fiscal Year 2024 Federal Information Security Modernization Act inventory.

[8] Our sample was selected using a 95 percent confidence interval, 10 percent error rate, and ±7.5 percent precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total is between 0 and 11.

Internal policies were not being followed to ensure the security of encryption keys

The IRS's servers containing encryption keys are located in limited access areas within its facilities. The access cards needed to log on to these servers are stored in locked cabinets. During our review, we found that the IRS did not follow its internal requirements to ensure that the encryption keys are secure.[9] Specifically, we found that the combinations for the cabinet locks were not changed as required. In addition, our auditors were allowed to enter limited access areas without signing the limited access area log at two IRS facilities. When the IRS fails to follow its processes to secure the limited access areas, it increases the risk of unauthorized access to the server with the encryption keys.

The Internal Revenue Manual (IRM) requires combinations and keys to cabinets to be changed every three years, when keys are lost or combinations are compromised, or when individuals are transferred or terminated. In addition, the IRM requires visitors to sign designated limited access area logs before entry.

According to personnel from the IRS's Enterprise Operation function, the cabinet locks were not changed because they were not aware of the IRS's requirement. In addition, personnel from the Facilities Management and Security Services function noted that despite its policy, TIGTA personnel are not required to sign to the limited access area logs when accessing the area. In November 2025, personnel from Facilities Management and Security Services stated that they are updating the IRM to require that all personnel sign in unless they are first responders during an emergency or on the Authorized Access List. The Authorized Access List includes people approved by the IRS's Facilities Management and Security Services function for unescorted or escorted physical access. It is also used in limited access areas to identify persons approved for unescorted access into designated limited access areas.

Management Action: After we identified the deficiency, personnel from the Information Technology Enterprise Operations function implemented procedures to change the combinations to the cabinet locks annually at the Memphis, Tennessee, and Kearneysville, West Virginia facilities and bi-annually at the other sites.

The majority of data are backed up but requests for data restoration were not resolved within the required time frames

The IRS is at the Initial level for data availability, *i.e.*, the IRS has data backup processes and data recovery procedures. To progress to the Advanced level of the Zero Trust Maturity Model, the agency must be able to make data available from redundant, highly available data stores and ensure access to historical data.

Both the IRM and NIST require the backup of user level information, system level information, and system documentation, including security-related documentation, for both on-premise and cloud systems.

- **Data backup processes.** IRS data are replicated to a secondary site to ensure the duplication of data. We reviewed 60 on-premise systems that contain critical data and found that 54 (90 percent) had evidence of backup for all data in the systems. However, 5 (8 percent) were not backed up and 1 (2 percent) system was partially backed up. We also reviewed 15 cloud systems that contain critical data and found that the IRS had

[9] Encryption keys are strings of characters that are used for altering data so that they appear random.

sufficient documentation to support backups by the cloud service providers for all 15 systems.

- **Data recovery procedures.** The IRS implemented recovery procedures for its on-premise systems in case of a system failure or loss of data. Users request to restore lost or corrupt data using a ticket request system and assign a priority for that request. However, our review determined that the IRS does not timely resolve restoration requests. We reviewed 1 high priority, 53 medium priority, and 27 low priority data recovery requests from October 2024 through March 2025 and found more than half of the medium and low priority restoration requests were not resolved within the required time frames.[10] Figure 2 below outlines the required time frames for data restoration for each priority level.

Figure 2: Data Recovery Priorities and Restoration Time Frames

Priority	Priority Description	Target Resolution Time
1	Critical	1 hour
2	High	4 hours
3	Medium	8 hours
4	Low	12 hours

Source: IRS Standard Operating Procedures for Tier 2 Backup.

In addition, the IRS reviews the data recovery procedures implemented by cloud service providers as part of its annual assessment. We reviewed the data recovery procedures for 15 cloud systems with critical data and found that 13 (87 percent) of 15 systems had an established recovery process and can restore data within the organization's defined time period. Two (13 percent) of the 15 systems did not have sufficient documentation for disaster recovery testing or have recovery procedures as required.

IRS officials stated that the delays in recovery were primarily due to the complexity and manual nature of performing the recovery tasks. In addition, they added that processing times are subject to adjustments or changes to recovery requests. Further, recovery timelines could increase due to delays in confirmation of successful recoveries. By not restoring the data in a timely manner, it could impact the ability of the IRS to conduct its business operations.

Recommendation 1: The Chief Information Officer should evaluate the current data restoration process and streamline processes, as needed, to ensure that data recovery timelines are met.

Management's Response: The IRS agreed with this recommendation. The Chief Information Officer will evaluate the current data restoration process and ensure that data recovery timelines are met.

Data governance bodies were created but were not included in the governance plans

During our review, we found that the IRS is at the Traditional level for data governance capability, *i.e.*, the IRS relies on *ad hoc* data governance policies with manual implementation. To

[10] Examples of medium priority requests we reviewed include requests to restore data from multiple files, folders or a drive. Low priority requests included requests to restore a single file or document.

advance to the Initial level of the Zero Trust Maturity Model, agencies must define high level data governance policies while relying primarily on manual, segmented implementation.

In July 2019, the OMB required the head of each agency to create an agency Data Governance Body to be chaired by the Chief Data Officer and include their data governance bodies in the Strategic Information Resources Management Plan's Governance sections by September 2019.[11] The IRS created two data governance bodies to meet this requirement.

- The Data and Analytics Strategic Integration Board was created in March 2019, with the mission to promote and enhance the application of data and analytics solutions to improve operations and mission effectiveness.
- The Data Security Executive Steering Committee was created in December 2023, with the mission to oversee the sustainability of data security practices and policies at the IRS.

Members of both governance bodies include, but are not limited to, the Chief Data Analytics Officer, the Chief Technology Officer, the Chief Privacy Officer, the Chief Financial Officer, the Associate Chief Information Officer, Enterprise Services, and the Deputy Chief Tax Compliance Officer for Strategy and Analytics.

During our review, the IRS presented different documents such as the Information Security Program Plan and the Inflation Reduction Act Strategic Operating Plan document as evidence of its governance plan. However, we found that the IRS did not include the governance boards in these documents as required. Furthermore, our interpretation of OMB Circular A-130 is that agencies are required to create a single strategic plan for managing and maintaining their information resources.[12] The IRS's use of different documents does not fulfill this requirement.

Recommendation 2: The Chief Information Officer should develop a single document to serve as its Information Resources Management Strategic Plan and ensure that the plan includes all required components as outlined in OMB Circular A-130.

> **Management's Response:** The IRS agreed with this recommendation. The Chief Information Officer will develop the Information Resources Management Strategic Plan after the IRS Strategic Plan is finalized and published (anticipated spring 2026) to ensure alignment with agency goals and objectives, consistent with the guardrails and framework in OMB Circular A-130.

[11] OMB, Memorandum M-19-23, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance* (July 2019).

[12] OMB, Circular A-130, *Managing Information as a Strategic Resource* (July 2016).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to assess the IRS's data governance strategy and to determine if the IRS effectively implemented key controls, processes, and planned deliverables related to the Zero Trust Maturity Model Data Pillar Functions. To accomplish our objective, we determined whether:

- The IRS implemented Data at Rest Encryption for all high value assets and critical systems by meeting with IRS personnel and reviewing documentation showing the encryption status of the high value assets and critical systems. We selected and reviewed all 13 high value assets and a statistically valid sample of 50 critical systems from a population of 149 critical systems. We relied on the TIGTA's contract and agency statisticians to verify our sampling methods, provide the statistical sample, and the projection. We selected our sample using a 95 percent confidence level, a ±7.5 percent precision factor, and a 10 percent estimated error rate.
- The IRS implemented Data Inventory Management by reviewing the list of possible data stores available for ingestion to the EDP and comparing that to the list of data stores currently in the EDP.
- The IRS implemented Data Categorization by interviewing IRS personnel, observing demonstrations of current capabilities, and reviewing sensitivity labels and settings.
- The IRS's data governance policies meet federal requirements and are effective in guiding the implementation of data inventory processes at the IRS by interviewing IRS personnel, reviewing governance board charters and meeting minutes, and obtaining information from the IRS on the status of different data governance projects.
- The IRS's physical security for encryption servers is effective by going on-site to test the process for gaining access to the encryption hardware and the login process for the encryption hardware.
- The IRS's process for backing up critical data is effective and complete by obtaining and reviewing evidence of recent backups for all 60 IRS critical on-premise systems containing critical data. In addition, we determined whether the IRS is ensuring that cloud providers are effectively backing up critical data for 15 cloud systems deemed to contain critical data. Further, we determined whether data recovery procedures are in place by reviewing recovery requests from October 2024 through March 2025.

Performance of This Review

This review was performed in the Enterprise Operations function located at the Memphis Enterprise Computing Center located in Memphis, Tennessee, and the Martinsburg Enterprise Computing Center located in Kearneysville, West Virginia, and with information obtained from the Applications Development, Cybersecurity, Enterprise Operations, and Enterprise Services functions during the period September 2024 through November 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 finding and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objective.

Data Validation Methodology

We performed tests to assess the reliability of data from the As Built Architecture, Data Encryption Tracking Spreadsheet, and a Mission Essential Function spreadsheet. We evaluated the data by 1) reviewing required data elements; 2) reviewing the data to detect obvious errors, duplicate values, and unexpected missing data; and 3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for the 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: OMB requirements, NIST guidance, and IRM policies. We evaluated these controls by interviewing IRS subject matter experts, testing the controls over physical access to secure computing areas and reviewing evidence of encryption of IRS systems.

Appendix II

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

March 6, 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: 2026.03.06 13:09:33 -05'00'

SUBJECT: Draft Audit Report – The IRS Has Made Limited Progress Implementing Zero Trust Data Principles (Audit #2025208013)

The IRS appreciates the opportunity to review and respond to the draft audit report. Despite initial progress, more work remains in the ongoing effort to fully mature the agency's Zero Trust capabilities consistent with federal guidelines.

Each year, we conduct a robust self-assessment to identify strengths, gaps, and opportunities to strategically deploy our resources in addressing the most pressing threats. We have already achieved an advanced maturity level in several functional areas not specifically detailed in this report and recognize that we have the greatest opportunity to strengthen capabilities associated with the data pillar. We concur with the recommendations and have included a corrective action plan.

The IRS values the continued support and partnership provided by your office. If you have any questions, please contact my office at (202) 317-5000, or a member of your staff may contact Courtney Williams, Coordinating Director, Strategy & Plan Management, at (409) 801-0209.

Attachment

Attachment

Audit #2025208013, *The IRS Has Made Limited Progress Implementing Zero Trust Data Principles*

Recommendations

RECOMMENDATION 1: The Chief Information Officer should evaluate the current data restoration process and streamline processes, as needed, to ensure that data recovery timelines are met.

CORRECTIVE ACTION 1: The IRS agrees with this recommendation. The Chief Information Officer will evaluate the current data restoration process and ensure data recovery timelines are met.

IMPLEMENTATION DATE: October 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Infrastructure

RECOMMENDATION 2: The Chief Information Officer should develop a single document to serve as its Information Resources Management Strategic Plan and ensure the plan includes all required components as outlined in OMB Circular A-130.

CORRECTIVE ACTION 2: The IRS agrees with this recommendation. The Chief Information Officer will develop the IRS Information Resources Management Strategic Plan after the IRS Strategic Plan is finalized and published (anticipated spring 2026) to ensure alignment with agency goals and objectives, consistent with the guardrails and framework in OMB Circular A-130.

IMPLEMENTATION DATE: December 15, 2026

RESPONSIBLE OFFICIAL(S): Coordinating Director, Strategy & Product Management

Appendix III

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.*
Data at Rest	Data that is not actively moving from device to device or network to network such as data stored on a hard drive, laptop, flash drive, or archived/stored in some other way.
Data Categorization	The practice of organizing and classifying data into different categories, groups, or segments.
Data Inventory Management	The process of cataloguing, categorizing, and managing an organization's data assets.
Data Loss Prevention	The practice of detecting and preventing confidential data and Personally Identifiable Information from being "leaked" out of an organization's boundaries, either intentionally or unintentionally.
Data Store	A digital repository that stores and safeguards the information in computer systems.
Encryption	The process of converting plain text to cipher text by means of a cryptographic system.
Enterprise Data Platform	A central repository to make data more accessible at the IRS by onboarding, storing, managing, and providing secure access to taxpayer and business data.
Federal Information Processing Standards	These are standards for federal computer systems that are developed by the National Institute of Standards and Technology and approved by the Secretary of Commerce in accordance with the Information Technology Management Reform Act of 1996 and Computer Security Act of 1987.
High Value Asset	Refers to those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical federal operations or house unique collections of data (by size or content) making them of particular interest to criminal, politically motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government.
Internal Revenue Manual	The primary source of instructions to employees relating to the administration and operation of the IRS. The manual contains the directions employees need to carry out their operational responsibilities.
Legacy Systems	An information system that may be based on outdated technologies but is critical to day-to-day operations. In the context of computing, it refers to outdated computer systems, programming languages, or application software that are used instead of more modern alternatives.

Term	Definition
On-Premise	On-premise refers to the use of a company's own servers and Information Technology environments on-site.
Tier I System	Supercomputers and mainframe hardware and software, including peripheral subsystems used in mainframe system environments.
Tier II System	Computers that usually contain multiple microprocessors, capable of executing multiple processes simultaneously.
Zero Trust Architecture	The implementation, practical application and design that enforces zero trust principles in an organization's Information Technology infrastructure.
Zero Trust Maturity Model	Assists agencies in the development of zero trust strategies and implementation plans. The maturity model, which includes five pillars, is based on the foundations of zero trust. Within each pillar, the maturity model provides specific examples of Traditional, Initial, Advanced, and Optimal zero trust architectures.

Appendix IV

Abbreviations

EDP	Enterprise Data Platform
IRM	Internal Review Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
TIGTA	Treasury Inspector General for Tax Administration
ZTA	Zero Trust Architecture

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.