TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk

September 27, 2022

Report Number: 2022-20-052

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

HIGHLIGHTS: Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk

Final Audit Report issued on September 27, 2022 **Report Number 2022-20-052**

Why TIGTA Did This Audit

Governmentwide mandates required Federal agencies to expand the use of shared services to enable broader use and adoption of cloud computing. Cloud computing is defined as the delivery of computing services, including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet to offer faster innovation, flexible resources, and economies of scale.

This audit was initiated to evaluate the effectiveness of controls to protect taxpayer data on cloud computing services.

Impact on Tax Administration

Control weaknesses over cloud computing services can pose a substantial risk to taxpayer records currently residing on these services. The potential harm includes breach and unauthorized access and disclosure of taxpayer information.

What TIGTA Found

To facilitate and guide its cloud security implementation efforts, the IRS developed its Cloud Security Reference Architecture in September 2019 and the Cybersecurity Cloud Operations Framework in November 2019. The IRS issued its updated Cloud Strategy and Cloud Security Internal Revenue Manual in March 2021 and September 2021, respectively.

By the end of Calendar Year 2020, the IRS had fully implemented 56 cloud services, 12 of which contained taxpayer data. The IRS deployed these cloud services without fully implemented security controls for protecting the data.

Encryption is a key control for protecting the taxpayer data on IRS cloud services. [redacted]

[redacted]

The IRS continues cloud deployments despite not having a fully implemented security control infrastructure in place.

What TIGTA Recommended

TIGTA recommended that the Chief Information Officer should (1) expedite full implementation of the cloud security control infrastructure, [redacted] and (2) develop an implementation plan for selected cloud capability gaps relating to identity and access management, data and infrastructure protection, continuous security monitoring, and program management.

The IRS partially agreed with the first recommendation, stating that it has a robust and comprehensive security control infrastructure documented within Internal Revenue Manuals for cloud implementations and will continue to ensure compliance with the documented cloud security control infrastructure for [redacted] However, the IRS has not fully implemented key security controls as outlined in our report. The IRS agreed with the second recommendation and plans to develop an implementation plan for selected cloud capability gaps.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 27, 2022

MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

FROM: Heather M. Hill
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Cloud Services Were Implemented Without Key Security Controls, Placing Taxpayer Data at Risk (Audit #202120004)

This report presents the results of our review to evaluate the effectiveness of controls to protect taxpayer data on cloud computing services. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS [Internal Revenue Service] Resources*.

Management's complete response to the draft report is included as Appendix III. During the course of this review, we had numerous meetings with the IRS to discuss the identified issues and to obtain their feedback. As a result, we made significant revisions to the draft report. In its response, the IRS states, "the audit team has implied that the IRS placed 12 systems containing taxpayer data into the cloud without performing a security assessment, which is inaccurate." We are not implying that the systems in the cloud lack security assessments but rather that key security controls were not fully implemented.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Background

Governmentwide mandates[1] required Federal agencies to expand the use of shared services to enable broader use and adoption of cloud computing. Cloud computing[2] is defined as the delivery of computing services,[3] including servers, storage, databases, networking, software, analytics, and intelligence, over the Internet to offer faster innovation, flexible resources, and economies of scale. In addition, these mandates direct the Federal Government to accelerate movement to secure cloud services. As part of its modernization efforts and to align with Federal mandates, the Internal Revenue Service (IRS) is engaged in a significant migration of services to the cloud.

One of the goals of this migration is to maintain application efficiency and overall service agility. The IRS plans to accomplish this by transitioning data, applications, and services from an on-site presence to the cloud environment. The IRS's Integrated Modernization Business Plan, dated April 2019, states that maintaining a cloud infrastructure will reduce the fixed investment and minimize the risks of aging hardware. The plan also states that cloud execution will result in improved "time to market" agility, increased operational efficiency and resilience, increased innovation, and an enhanced or maintained security posture by migrating workloads to cloud platforms and services.

The IRS first implemented cloud services in Calendar Year 2014. By October 2018, the IRS had placed 17 services in the cloud. By the end of Calendar Year 2020, the IRS had 56 services operating in the cloud. The IRS identified another 253 potential cloud candidates for migration in one to three years.

While cloud deployments can bring many operational benefits to an organization, security control weaknesses over cloud computing services can pose a substantial risk to the data residing on these services. For IRS cloud deployments, these data include taxpayer data. The potential harm includes breach and unauthorized access to and disclosure of taxpayer data. To illustrate the risk, one recent study[4] concluded that cloud breaches[5] in Calendar Years 2018 and 2019 exposed nearly 33.4 billion records and cost companies nearly $5 trillion. Gartner Inc.[6]

---

[1] Governmentwide mandates include the Federal Cloud Computing Strategy *("Cloud First" and "Cloud Smart")* (Feb. 8, 2011, and June 24, 2019, respectively); Office of Management and Budget Memoranda M-16-19, *Data Center Optimization Initiative* (Aug. 1, 2016), and M-19-19, *Update to Data Center Optimization Initiative* (June 25, 2019); and Executive Orders 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), and 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).

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

[3] For consistency throughout our report, we will generally use the term 'service' or 'services' rather than 'application' or 'system.' This is the most appropriate term to use in this report for consistency.

[4] DivvyCloud 2020 Cloud Misconfigurations Report (February 18, 2020).

[5] Office of Management and Budget Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (Jan. 3, 2017), defines a 'breach' as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person, other than an authorized user accesses or potentially accesses Personally Identifiable Information or (2) an authorized user accesses or potentially accesses Personally Identifiable Information for an other-than-authorized purpose.

[6] Gartner Inc. is a research and advisory company that delivers technology-related insights to its clients to help them make the right decisions.

estimated that the worldwide public cloud services market was $182.4 billion in Calendar Year 2018 and $214.3 billion in Calendar Year 2019. This means that the cost to companies due to cloud breaches is more than 12 times the amount of worldwide investments in cloud services. Companies must ensure effective cloud security in order to protect their investments and prevent devastating costs associated with data breaches.

IRS cloud implementations and security activities

In late Calendar Year 2019, after 23 cloud services were fully implemented, the IRS identified critical challenges in its cloud environment and the need for a security structure that handles the whole cloud ecosystem, referred to as a "cloud security control infrastructure."[7] At that time, the IRS initiated actions to design and implement this infrastructure. A cloud security control infrastructure that supports an organization's entire cloud ecosystem helps reduce the attack surface of that ecosystem. Conversely, a piecemeal approach to cloud security can expand the attack surface and increase risk. Therefore, a fully implemented cloud security control infrastructure is vital for protecting taxpayer information in the cloud.

To facilitate and guide its cloud security implementation efforts, the IRS developed its Cloud Security Reference Architecture in September 2019 and Cybersecurity Cloud Operations Framework in November 2019. The IRS also issued its updated Cloud Strategy and a cloud security–specific Internal Revenue Manual (IRM)[8] in March 2021 and September 2021, respectively. In addition to establishing numerous security controls, the IRS indicated that it performed the following security-related activities as of June 2021:

- The Cybersecurity function established the Cloud Security Assessment and Authorization Program in July 2019. The Cybersecurity Security Risk Management team has performed a variety of initial, event-driven, and annual security assessments for cloud projects.
- The Cybersecurity function identified tools within the Cybersecurity Inventory of Tools and Technologies that support the IRS's migration to the cloud and outlined the variety of service and deployment models and the capability areas that these tools support. It also identified and prioritized approximately 60 tools for cloud migration based on tool complexity and business benefit analysis.
- The IRS established the Cybersecurity Cloud Program Management Office in November 2019 to provide project management and oversight for the deployment of Cybersecurity tools. The mission of the Cybersecurity Cloud Program Management Office is to operate, maintain, and enhance existing cybersecurity systems, programs, projects and the existing tools suite.
- The IRS continued to perform analysis for implementing and adopting capabilities to manage encryption keys and protect data in transit and at rest across the IRS's future hybrid multicloud information technology environment. The Cyber Cloud Team drafted a Key Management System whitepaper to detail the approach for the management and

[7] We use the term 'cloud security control infrastructure' to represent a comprehensive set of controls applicable across the IRS's entire cloud ecosystem as well as to draw a distinction between controls implemented as part of a broad security strategy versus controls implemented in a service-by-service or piecemeal approach.

[8] IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* (Sept. 2021).

storage of encryption keys across the enterprise for cloud-based services, which included an analysis of scenarios whereby the IRS is and is not the originator of the master keys.

- The Cybersecurity function assisted project teams and Cyber Cloud stakeholders to address key cybersecurity requirements and support the organizational readiness of applications to migrate to the cloud and identify opportunities to involve the Cybersecurity function earlier in the cloud intake process.
- The Cyber Cloud Team researched the enterprise-wide understanding of the Federal Risk and Authorization Management Program (FedRAMP) and determined that educational efforts were needed. It hosted presentations and various meetings to collect information from stakeholders. This effort culminated in building a reusable process for the IRS's FedRAMP Initial Authorizing Agency efforts.
- The Cyber Cloud Executive Office led two separate cloud literacy discussions that resulted in baselining cloud knowledge across the group. Common terms and trends were defined and discussed, including the tie-in of relevant topics such as common security controls, FedRAMP, *etc*.
- The IRS used the Cloud Authorization Playbook to advise project teams on the Cybersecurity function's processes, artifacts, and procedures throughout the Enterprise Life Cycle. The playbook provides extensive information and details on how to get a purchased and FedRAMP-approved service into the IRS environment in a safe and secure manner. The playbook is updated regularly or when material changes occur to policies or processes.

Results of Review

Despite the aforementioned security activities surrounding its cloud services deployments, the IRS continued to accelerate cloud adoption without ensuring that important security controls designed to protect taxpayer data were in place in the cloud environment.

Taxpayer Data Were Stored on Cloud Services Without a Fully Implemented Security Control Infrastructure in Place

Key security controls were not implemented prior to placing taxpayer data in the cloud

The IRS Memorandum[9] regarding sensitive data states that all system deployments into cloud-hosted environments must comply with the requirements identified in IRMs 10.8.24 and 10.5.1.[10] The Department of the Treasury's Cloud-First guidance is to identify and mitigate cybersecurity risk prior to migrating workloads to the cloud.[11] Executive Order 14028 on Improving the Nation's Cybersecurity requires strict control over cloud services. The Executive

[9] IRS Memorandum, *Sensitive Data on Cloud-Hosted Systems* (Nov. 15, 2019). The only exception to the requirement is that the requisite authorization and/or risk acceptance has been obtained based on the current IRS and Federal policies.

[10] IRM 10.5.1, *Privacy and Information Protection, Privacy Policy* (Sept. 2019).

[11] Treasury Cloud Strategy Migration Framework (Aug. 7, 2017).

Order states that the Government must accelerate securing cloud services. Also, agencies shall adopt encryption to the maximum extent.

The Federal Cloud Computing Strategy[12] states that agencies should use a risk-based approach in securing their cloud environment. The Strategy emphasizes that agencies should use data-level protections that include the implementation of encryption and modern Identity, Credential, and Access Management controls. In addition, it is essential that agencies perform continuous monitoring to detect malicious activity.

As previously stated, the IRS is in the process of implementing a security control infrastructure to support all cloud systems and migrations. We identified security controls that are part of that infrastructure but are not in place. [redacted] and has implemented cloud services with known capability gaps. Although these controls apply to all cloud services, the risk related to not fully implementing these controls on the 12 cloud services with taxpayer data is greater due to the sensitivity of the data. When we presented these issues to the Cybersecurity executives, they agreed that the IRS needs to expeditiously implement a cloud security control infrastructure. Without a standardized cloud security control infrastructure in place, the risk of unauthorized access to taxpayer data increases.

The IRS [redacted]

The National Institute of Standards and Technology (NIST)[13] requires that cryptographic (*i.e.,* encryption)[14] keys are established and managed. Encryption keys are strings of characters used within an encryption algorithm for altering data so that they appear random. Like a physical key, it locks (encrypts) data so that only someone with the right key can unlock (decrypt) them.

[redacted][15] [redacted][16] [redacted][17] [redacted]

[12] The June 2019 Federal Cloud Computing Strategy — Cloud Smart is a long-term, high-level strategy to drive cloud adoption in Federal agencies.

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

[14] The NIST defines "encryption" as the cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent them from being known or used. Therefore, "cryptographic" is equivalent to "encryption," and we use the terms interchangeably.

[15] We used the terms "cloud vendor" and "cloud service provider" interchangeably.

[16] [redacted]

[17] [redacted]

[redacted]

The NIST[18] advocates logging any activity related to keys, including their generation, access, modification, revocation, or destruction. In addition, the NIST requires the auditing of activities associated with key management. On a more frequent basis, the actions of the entities that use, operate, and maintain the system should be reviewed to verify that they continue to follow established security procedures and have accessed only those keys for which they are authorized. This is normally accomplished by examining the logs created to record security-relevant events. The NIST further states that strong encryption systems can be compromised by lax and inappropriate actions. Highly unusual events should be noted and reviewed as possible indicators of attempted attacks on the system. In addition, the IRM requires that the IRS reviews and analyzes information systems' audit records at least weekly for indications of inappropriate or unusual activity and reports findings at a minimum to the Information System Security Officer.

[redacted]

The IRS [redacted]

IRM 10.8.24 states that the information system shall generate audit records containing event information that establishes what type, when, where, the source, the outcome, and the identity

[18] NIST, Special Publication 800-57, Part 1, Revision 5, *Recommendation for Key Management: Part 1 – General* (May 2020).

of any individuals or subjects associated with the event. IRM 10.8.1 requires that IRS systems generate audit records with details to facilitate the reconstruction of events if an unauthorized activity or a malfunction occurs or is suspected. The IRM 10.5.5[19] states that the Cybersecurity function is responsible for reviewing and certifying various data security reports. It must analyze and partner with management to determine the validity of account-related accesses.

In general, Internal Revenue Code § 6103 requires that tax returns and return information be confidential. In addition, the Taxpayer Browsing Protection Act of 1997[20] placed an additional responsibility on the IRS to protect taxpayer information from the willful unauthorized access, attempted access, or inspection of taxpayer returns or return information (also referred to as UNAX). For each IRS system or service containing taxpayer data, whether on-premise or in the cloud, the IRS is required to obtain and review complete and accurate transactional data in order to properly administer its UNAX responsibilities. UNAX audit trails and the related monitoring help detect if taxpayer data were accessed for unauthorized purposes and ensure compliance with Federal law.

[redacted][21][22]

The IRS implemented cloud services with known capability gaps that remain in the areas of identity and access management, continuous security monitoring, data and infrastructure protection, and program management and integration

The security requirements within IRM 10.8.24 and IRM 10.8.1 must be met for cloud services to satisfy Federal Information Security Modernization Act of 2014[23] compliance, which includes information technology security controls for identity and access management, continuous security monitoring, data and infrastructure protection, and program management.

[19] IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements* (July 2018).

[20] Pub. L. No. 105-35, 26 U.S.C. §§ 7213, 7213A, 7431.

[21] [redacted]

[22] [redacted]

[23] Pub. L. No. 113-283.

The Treasury Cloud Strategy Migration Framework[24] affirms a gap analysis should be conducted comparing existing information technology capabilities[25] with those required by the future state. Strengths should be highlighted to ensure that they are not compromised when developing the cloud strategy. Weaknesses and gaps should be assessed for opportunities to strengthen or fill needed capabilities using cloud technologies. These opportunities should then be prioritized based on overall feasibility and value.

In late Calendar Year 2019, after 23 cloud services had been fully implemented, the IRS reviewed three applications containing taxpayer data hosted in moderate cloud environments to provide a baseline for the current state of the IRS cloud environment. The IRS also used stakeholders and documentation reviews and assessed the cloud current state against IRM policies,[26] NIST Special Publication 800-53 controls, and identified gaps. The gaps the IRS identified are security capabilities required to operate in the cloud as a consumer. These capabilities could apply to all cloud services with taxpayer data.

The IRS subsequently presented many of these cloud capability gaps in its migration plan, along with initiatives to address them. Due to the number of capability gaps, we presented only selected examples by security area. However, all the cloud capabilities the IRS identified play a role in protecting taxpayer data in the cloud. Appendix II provides a list of the IRS-identified cloud capability gaps.

Identity and access management

- No integration of authorized cloud-based applications with Active Directory Federation Services.[27]
- No implementation of short-term identity architecture and design.

Continuous security monitoring

- No fully implemented incident management processes.
- No fully defined and implemented plan to integrate native cloud services with on-premise tools for network monitoring.

Data and infrastructure protection

- No defined and implemented clear key escrow[28] and recovery processes to mitigate data loss risks.
- No defined roles and responsibilities for management of encryption key life cycle.

[24] Treasury Cloud Strategy Migration Framework (Aug. 7, 2017).

[25] The NIST defines "capability" as a combination of mutually reinforcing security and/or privacy controls implemented by technical, physical, and procedural means. Such controls are typically selected to achieve a common information security- or privacy-related purpose.

[26] IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* (May 2019); IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* (March 2019); and IRM 10.5.1, *Privacy and Information Protection, Privacy Policy* (Sept. 2019).

[27] Active Directory Federation Services capability is required by the IRS for Homeland Security Presidential Directive 12 compliance. The IRS confirmed that at least 38 cloud services do not have this capability and, as such, are not compliant.

[28] The NIST defines "key escrow" as the retention of the private component of the key pair associated with a subscriber's encryption certificate to support key recovery.

Program management and integration

- No roadmaps for implementation of core cloud security solutions.
- No training or hiring plans to fill Cybersecurity function cloud workforce gaps.

[redacted]

The President's Executive Order 14028 on Improving the Nation's Cybersecurity states that prevention, detection, assessment, and remediation of cybersecurity incidents is a top priority. As cloud services are implemented, agencies must do so in a deliberate way in order to help prevent, detect, assess, and remediate cyber incidents.

As previously stated, the IRS is responsible for protecting taxpayer information from the willful unauthorized access, attempted access, or inspection of taxpayer returns or return information referred to as UNAX. The IRM states that the Cybersecurity function shall manage a centralized evaluation capability to identify potential UNAX violations. Because Federal law requires taxpayer information to be monitored to prevent UNAX and general browsing of taxpayer information, the IRS is required to monitor the activity where these data reside to prevent such UNAX.[29]

[redacted][30]

[29] Audit and Accountability Strategy for IRS Information Systems Hosted in the Cloud (July 16, 2020).

[30] [redacted]

[redacted]

[redacted][31]

[redacted]

The acceleration of cloud deployments coupled with not having a fully implemented cloud security control infrastructure in place prior to turning over control of taxpayer data to the CSPs limits management's ability to fully provide the necessary assurance to protect taxpayer data.

The Chief Information Officer should:

Recommendation 1: Expedite full implementation of the cloud security control infrastructure, [redacted]

Management's Response: The IRS partially agreed with this recommendation. The IRS has a robust and comprehensive security control infrastructure documented within IRM 10.8.1 and 10.8.24 for cloud implementations. The IRS will continue to ensure compliance with the documented cloud security control infrastructure for increased CSP key management monitoring, including enhancement of audit trails.

Office of Audit Comment: The IRS's corrective action does not address the intent of our recommendation. The IRS has security control policies for cloud implementations documented within IRM 10.8.1 and 10.8.24. However, the IRS has not fully implemented key security controls as outlined in our report. [redacted] and has implemented cloud services with known capability gaps. Since the IRS currently

[31] [redacted]

has systems in the cloud, the implementation of necessary security controls, including [redacted] should be expedited.

Recommendation 2: Develop an implementation plan for selected cloud capability gaps relating to identity and access management, data and infrastructure protection, continuous security monitoring, and program management.

Management's Response: The IRS agreed with this recommendation. The Information Technology organization will develop an implementation plan for selected cloud capability gaps relating to identity and access management, data and infrastructure protection, continuous security monitoring, and program management.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of controls to protect taxpayer data on cloud computing services. To accomplish our objective, we:

- Obtained an understanding of the processes to ensure that security controls are maintained on cloud services by interviewing IRS management and personnel and reviewing Federal Government and IRS requirements and documentation that specifically addressed the security of cloud services.
- Identified the number of cloud services used by the IRS from monthly cloud security reports and determined which cloud services contained taxpayer data.
- Determine whether the IRS established and implemented a comprehensive set of security controls for cloud services to ensure that sensitive data are protected against unauthorized access and use by interviewing IRS management and personnel and reviewing documentation.

Performance of This Review

This review was performed with information obtained from the IRS's Information Technology organization located in New Carrollton, Maryland, during the period September 2020 through January 2022. 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); Kent Sagara, Director; Jason McKnight, Director; Joseph Cooney, Audit Manager; Bret Hunter, Lead Auditor; and Esther Wilson, Senior Auditor.

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: IRM 10.8.1, *Information Technology Security, Policy and Guidance* (May 9, 2019, and September 28, 2021); IRM 10.8.24, *Information Technology Security, Cloud Computing Security Policy* (March 20, 2019, and September 28, 2021); NIST Special Publication 800-53; and controls identified in various other NIST and industry sources. We evaluated these controls by interviewing Information Technology organization personnel and reviewing available documentation.

Appendix II

IRS-Identified Cybersecurity Cloud Capability Gaps

This appendix presents detailed information on the IRS-identified capability gaps in its current cloud security environment. These gaps formed the basis for the Cybersecurity Cloud Key Initiatives in the IRS Cloud Security Roadmap and the Cyber Migration Plan.

The capability gaps outlined below represent the Cyber Cloud Executive Office's understanding of the current security capabilities required to operate in the cloud as a consumer. These capability gaps have been determined as a result of a NIST Special Publication 800-53 assessment based on conversations with project teams and Cybersecurity function stakeholders and a review of relevant documentation. The weaknesses and gaps listed are not meant to be an all-inclusive list of capabilities that are not in place.

Key initiative areas and capability gaps

Continuous Security Monitoring

- No fully implemented incident management processes to address CSP service model scenarios.
- No fully defined and implemented plan for vulnerability scanning in cloud.
- No fully defined and implemented plan for cloud-based server image life cycle management and compliance enforcement process.
- No fully defined and implemented plan to modify security change management process to support automated remediation.
- No fully defined and implemented plan to identify and implement threat and vulnerability management tool requirements for multiple platforms.
- No fully defined and implemented plan to integrate container scanning[1] into continuous integration and continuous delivery pipeline.
- No fully defined and implemented plan to address penetration testing requirements across CSPs.
- No fully defined and implemented plan to transition to a third-party SaaS tool for vulnerability and configuration policy compliance management across CSPs.
- No defined use cases and requirements and no configured functionality to support user behavior analytics.
- No fully defined and implemented plan to transition from legacy tools for user behavior analytics.

[1] The NIST defines "container" as a method for packaging and securely running an application within an application virtualization environment. Container scanning is the process of scanning containers and their components to identify potential security threats.

- No fully defined and implemented plan to integrate native cloud services with on-premise tools for network monitoring.

Identity and Access Management

- No defined potential privileged access management use cases in cloud based upon analysis of on-premise infrastructure and projected migration priorities.
- No architected and designed short-term and long-term identity infrastructures in cloud to support projected privileged access management use cases, including initiating procurement of long-term identity solution.
- No readiness determination of identity and access management solution to support privileged access management use cases in cloud.
- No defined and executed plan to mitigate/resolve organization readiness challenges.
- No implemented processes to discover cloud applications currently accessed by IRS users outside Active Directory Federated Services.
- No defined remediation plan to control all cloud-based application access via Active Directory Federated Services.
- No implementation of short-term identity architecture and design for cloud.
- No integration of authorized cloud-based applications with Active Directory Federation Services.
- No verification of process to integrate new cloud-based applications with Active Directory Federated Services for nonprivileged and privileged user access provisioning, authentication, and authorization.
- No testing of implementation and integration of two to three new cloud-based applications with Active Directory Federated Services and identity and access management solution.
- No modification of existing processes to integrate new cloud-based applications with Identity as a Service solution.

Data and Infrastructure Protection

- No implementation of identity and access management solution for encryption key management recertification process.
- No defined roles and responsibilities for key users and stakeholders.
- No implementation of solution for "bring your own key" for encryption of data at rest and in transit.
- No defined and implemented standardized approach for prototyping and validating Key Management System processes into cloud projects.
- No developed and integrated automation process for identifying and revoking expired/compromised keys.
- No integration of Cloud Project Management Office Service Catalog Key Management System solutions into standard intake for new cloud projects.

- No defined and implemented clear key escrow and recovery processes to mitigate data loss risks.
- No defined roles and responsibilities for management of key life cycle (*e.g.,* generation, deployment, retirement).

Program Management and Integration

- No roadmaps for implementation of core cloud security solutions (Continuous Security Monitoring, Identity and Access Management, Encryption Key Management).
- No communication plan with key stakeholders to familiarize project teams with core cloud security solutions.
- No execution on defined implementation plans for core cloud security solutions.
- No Software Catalogue to provide a list of preapproved CSP products and services for project teams to select from.
- No analysis of acquisition process to determine how non-FedRAMP cloud services are being procured without proper Cybersecurity function review/approval.
- No updated acquisition process to incorporate FedRAMP certification considerations before procurement.
- Inadequate guidance on Security Change Management process.
- No Cyber Cloud Workforce skills assessment to identify potential gaps in resources and/or knowledge.
- No training and/or hiring plans to fill Cybersecurity function cloud workforce gaps.
- No execution of training and/or hiring plans.

Appendix III

Management's Response to the Draft Report

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

CHIEF INFORMATION OFFICER

September 13, 2022

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger /s/ Nancy A. Sieger
Chief Information Officer

SUBJECT: Draft Audit Report – Cloud Services Were Implemented Without Key Security Controls Placing Taxpayer Data at Risk
(Audit # 202120004)

Thank you for the opportunity to review the draft audit report. We are once again disappointed that the IRS and the TIGTA audit team proved unable to correct and improve the audit report at the discussion draft stage. Unfortunately, this draft audit report does not accurately reflect the agency's cloud security posture and also includes several misleading statements without appropriate context. The IRS continues to make progress deploying secure cloud services and we have a detailed corrective action plan to make additional process improvements.

Throughout this audit, the IRS provided the audit team corrections to several unsubstantiated claims and mischaracterizations that have been included in the draft audit report. For example, the audit team has implied that the IRS placed 12 systems containing taxpayer data into the cloud without performing a security assessment, which is inaccurate. As standard practice, we perform security assessments of all cloud systems; we document and maintain the associated security artifacts; and we track and manage and monitor risk. For any security controls not fully in place, the IRS relies on a mature risk management process for risk-based decision making. Furthermore, we employ multiple layers of protection against threats to IRS processes, facilities, systems, data, and technology, and we have a mature cybersecurity program in place to protect data in the cloud from unauthorized use and disclosure.

[redacted]

In conclusion, the IRS has a robust and comprehensive security control infrastructure in place for cloud implementations (see IRM 10.8.1 and 10.8.24). The IRS appreciates our continued partnership with TIGTA, and we are committed to continuously improving our cloud security posture.

If you have any questions, please contact me at 202-317-5000 or a member of your staff may contact Anthony Gillespie, Acting Director, Cybersecurity Security Risk Management at 240-613-2834.

Attachment

Attachment

Draft Audit Report – Cloud Services Were Implemented Without Key Security Controls Placing Taxpayer Data at Risk (Audit #202120004)

RECOMMENDATION 1:

The Chief Information Officer should expedite full implementation of the cloud security control infrastructure, [redacted]

CORRECTIVE ACTION #1:
The IRS partially agrees with this recommendation. IRS has a robust and comprehensive security control infrastructure documented within IRM 10.8.1 and 10.8.24 for cloud implementations. IRS will continue to ensure compliance with the documented cloud security control infrastructure for increased Cloud Service Provider (CSP) key management monitoring, including enhancement of audit trails.

IMPLEMENTATION DATE: October 15, 2024

RESPONSIBLE OFFICIALS:

Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress monthly until completion.

RECOMMENDATION 2: The Chief Information Officer should develop an implementation plan for selected cloud capability gaps relating to identity and access management, data and infrastructure protection, continuous security monitoring, and program management.

CORRECTIVE ACTION #2:
The IRS agrees with this recommendation. IT will develop an implementation plan for selected cloud capability gaps relating to identity and access management, data and infrastructure protection, continuous security monitoring, and program management.

IMPLEMENTATION DATE: September 15, 2023

RESPONSIBLE OFFICIALS:

Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN:
We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and review remediation progress monthly until completion.

Appendix IV

Glossary of Terms

Term	Definition
Attack Surface	The IRS As-Built Architecture defines an attack surface as the sum of all possible ways that an application or software product, service, Application Programming Interface, or any network-connected resource or device can be exploited by attackers.
Audit Trail	A chronological record of information service activities that is sufficient to permit reconstruction, review, and examination of a transaction from inception to final results.
Cloud Computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (*i.e.,* network, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud Ecosystem	A complex service of interdependent components that all work together to enable cloud services. In cloud computing, the ecosystem consists of hardware and software as well as cloud customers, cloud engineers, consultants, integrators, and partners. The IRS has a multicloud ecosystem comprised of cloud operations, cloud services, and cloud security.
Cloud Service Provider	An entity offering cloud-based platform, infrastructure, application, or storage services.
Control	A process effected by an entity's oversight body, management, and other personnel that provides reasonable assurance that the objectives of an entity will be achieved. It comprises the plans, methods, policies, and procedures used to fulfill the mission, strategic plan, goals, and objectives of the entity. It also serves as the first line of defense in safeguarding assets.
Cybersecurity	A function within the IRS Information Technology organization responsible for ensuring compliance with Federal statutory, legislative, and regulatory requirements governing confidentiality, integrity, and availability of IRS electronic systems, services, and data.
Data at Rest	In the context of data handling services, data at rest refers to data that are being stored in stable destination services. Data at rest are frequently defined as data that are not in use or are not traveling to service endpoints, such as mobile devices or workstations.
Data Breach	The potential or actual loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations in which persons other than authorized users and for other than authorized purposes have access or potential access to Personally Identifiable Information, whether physical or electronic.

Term	Definition
Encryption	The process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Enterprise Life Cycle	A structured business systems development methodology that requires the preparation of specific work products during different phases of the development process. The Enterprise Life Cycle establishes a set of repeatable processes and system of reviews, checkpoints, and milestones that reduce the risks of system development and ensure alignment with the overall business strategy.
Federal Risk and Authorization Management Program (FedRAMP)	A Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Hardware Security Module	A physical device that provides extra security for sensitive data.
Identity and Access Management	Provides direction for all development activities for external authentication and authorization as well as technical integration and coordination of other public facing applications in support of the Information Technology organization's secure data access activities, both within the IRS and with other Government agencies.
Infrastructure	The hardware, software, and network resources and services required for the existence, operation, and management of an enterprise information technology environment. It allows an organization to deliver information technology solutions and services to its employees, partners, and customers and is usually internal to an organization and deployed within owned facilities.
Internal Revenue Manual	The primary, official source of IRS instructions to staff related to the organization, administration, and operation of the IRS.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal agency operations and assets.
Plan of Action and Milestones	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Risk	A potential event that could have an unwanted impact on the cost, schedule, business, or technical performance of an information technology program, project, or organization.
Risk Management	The process of identifying, monitoring, and mitigating project and program risks.

Term	Definition
Security	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information services. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.
[redacted]	[redacted]
Software as a Service	The capability to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser, *e.g.,* web-based e-mail, or a program interface. The consumer does not manage or control the underlying cloud infrastructure (including network, servers, operating systems, storage, or even individual application capabilities), with the possible exception of limited user-specific application configuration settings.
Unauthorized Access	The willful unauthorized access, attempted access, or inspection of taxpayer returns or return information.

Appendix V

Abbreviations

CSP	Cloud Service Provider
FedRAMP	Federal Risk and Authorization Management Program
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
SaaS	Software as a Service
[redacted]	[redacted]
UNAX	Unauthorized Access

To report fraud, waste, or abuse,
call our toll-free hotline at:

(800) 366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration

P.O. Box 589

Ben Franklin Station

Washington, D.C. 20044-0589

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