



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere
to Federal Policy When Deploying a Cloud
Service*

August 7, 2017

Reference Number: 2017-20-032

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



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

1-800-366-4484

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.



HIGHLIGHTS

THE INTERNAL REVENUE SERVICE DOES NOT HAVE A CLOUD STRATEGY AND DID NOT ADHERE TO FEDERAL POLICY WHEN DEPLOYING A CLOUD SERVICE

Highlights

Final Report issued on August 7, 2017

Highlights of Reference Number: 2017-20-032 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

In December 2010, the U.S. Chief Information Officer directed all Federal agencies to shift to a “cloud first” policy. Not having a documented enterprise-wide cloud strategy creates a significant risk that organizations outside of the IRS Chief Information Officer and Information Technology organization may deploy systems and potentially expose Federal tax information with no reasonable assurance that the systems meet applicable Federal security guidelines. The IRS may also miss the opportunity to deliver public value by increasing operational efficiency and responding faster to constituent needs.

WHY TIGTA DID THE AUDIT

This audit was initiated to review the IRS’s progress in establishing an enterprise-wide cloud strategy and its compliance with Federal and agency guidelines and best practices. The overall objective was to review the IRS cloud strategy and how it has been implemented.

WHAT TIGTA FOUND

The IRS does not have an enterprise-wide cloud strategy. Although the IRS formed a working group in July 2016 to develop this strategy, it is not complete and no timeline has been established for completion.

The IRS inventory of cloud systems is updated manually when Change Management Requests are submitted. The inventory does not distinguish between deployed systems or systems in development, system ownership, or other informative details.

The IRS did not comply with Office of Management and Budget guidance that agencies use the Federal Risk and Authorization Management Program to conduct risk assessments, perform security authorizations, and grant Authorities to Operate for cloud services. The IRS began using a public cloud service in Calendar Year 2016 to allow public access to certain Form 990, *Return of Organization Exempt From Income Tax*, data. The Form 990 is required for tax-exempt organizations, nonexempt charitable trusts, and Section 527 political organizations to ensure that they comply with the tax law.

The Form 990 cloud project, which spanned more than a 20-month period, was implemented with limited involvement from the IRS Information Technology organization. In October 2015, the Tax Exempt and Government Entities Division discussed the Form 990 project with the Associate Chief Information Officer for Enterprise Services. However, the Tax Exempt and Government Entities Division was not instructed to appoint an authorizing official, generate an agency Authority to Operate letter, or to incorporate service level agreements within the cloud service user agreement.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer: 1) prioritize and complete an enterprise-wide cloud strategy in alignment with Federal guidance; 2) ensure that the process of managing the IRS’s cloud inventory is formalized using automated methods and updated on a periodic and ongoing basis; 3) designate an authorizing official, complete the Federal Risk and Authorization Management Program Security Assessment Report, and issue an agency-specific Authority to Operate letter for the Form 990 cloud service; and 4) ensure that the Form 990 cloud service includes a service level agreement.

The IRS agreed with two recommendations, partially agreed with one recommendation, and disagreed with one recommendation. The IRS did not agree with the recommendation that service level agreements were necessary for the Form 990 cloud service because its data are meant for public access.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 7 2017

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Does Not Have a
Cloud Strategy and Did Not Adhere to Federal Policy When Deploying
a Cloud Service (Audit # 201620021)

This report presents the results of our review of the Internal Revenue Service (IRS) cloud strategy and how it has been implemented. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Improving Tax Systems and Expanding Online Services.

Management's complete response to the draft report is included as Appendix V.

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, Acting Assistant Inspector General for Audit (Security and Information Technology Services).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Table of Contents

Background	Page 1
----------------------------------	--------

Results of Review	Page 3
---	--------

The Internal Revenue Service Does Not Have an Enterprise-Wide Cloud Strategy	Page 3
--	--------

Recommendations 1 and 2:	Page 5
--	--------

The Internal Revenue Service Did Not Follow Federal and Agency Cloud Service Guidelines for the Form 990 Cloud Project	Page 6
--	--------

Recommendations 3 and 4:	Page 10
--	---------

Appendices

Appendix I – Detailed Objective, Scope, and Methodology	Page 12
---	---------

Appendix II – Major Contributors to This Report	Page 13
---	---------

Appendix III – Report Distribution List	Page 14
---	---------

Appendix IV – Glossary of Terms	Page 15
---	---------

Appendix V – Management’s Response to the Draft Report	Page 19
--	---------



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Abbreviations

FedRAMP	Federal Risk and Authorization Management Program
IRM	Internal Revenue Manual
IRS	Internal Revenue Service



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Background

In December 2010, the U.S. Chief Information Officer released the *25 Point Implementation Plan to Reform Federal Information Technology Management*.¹ This plan was the culmination of 18 months of research and engagement with Federal information technology, acquisition, and program management communities; industry experts; and academics. Additional feedback was received from the U.S. Congress, Federal agency Chief Information Officers, and Federal Senior Procurement Executives. Placing an emphasis on cloud technologies, this 25-point plan was developed to deliver more value to the American taxpayer. The 25-point plan noted that active involvement from Federal agency leadership is critical to the success of these reforms.

In February 2011, the U.S. Chief Information Officer characterized the Federal Government's information technology environment as having low asset utilization, a fragmented demand for resources, duplicative systems, environments which are difficult to manage, and long procurement lead times.² These inefficiencies negatively affect the Federal Government's ability to serve the American public. The cloud computing model can significantly help agencies grappling with the need to provide highly reliable, innovative services quickly despite constrained resources. Cloud computing holds tremendous potential for the Federal Government to deliver public value by increasing operational efficiency and responding faster to constituent needs.

In September 2011, the National Institute of Standards and Technology³ reported that cloud computing is a model for enabling ubiquitous, 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 service provider interaction.⁴ Several benefits of cloud computing are increased scalability, on-demand services, energy efficiency, resource pooling, and metered services. The three service models used to define all cloud computing environments are Software As a Service, Platform As a Service, and Infrastructure As a Service. For each of the service models, there are four deployment models: Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud.

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, and the Internal Revenue Service (IRS) field office in Brooklyn, New York, during the period October 2016 through February 2017 with personnel from the Information Technology

¹ The White House, U.S. Chief Information Officer Vivek Kundra, *25 Point Implementation Plan to Reform Federal Information Technology Management* (Dec. 2010).

² The White House, U.S. Chief Information Officer Vivek Kundra, *Federal Cloud Computing Strategy* (Feb. 2011).

³ See Appendix IV for a glossary of terms.

⁴ National Institute of Standards and Technology, Special Publication 800-145, *The National Institute of Standards and Technology Definition of Cloud Computing* (Sept. 2011).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

organization's Enterprise Operations, Cybersecurity, and Enterprise Services organizations, and the Tax Exempt and Government Entities Division. 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. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Results of Review

The Internal Revenue Service Does Not Have an Enterprise-Wide Cloud Strategy

In December 2010, the U.S. Chief Information Officer released the *25 Point Implementation Plan to Reform Federal Information Technology Management*. Within this plan lies an overall objective for Federal agencies to shift to a cloud first policy. In addition, each agency is required to identify three “must move” services and create a plan for migrating into a cloud—one within 12 months and the remaining two within 18 months.

In February 2011, the U.S. Chief Information Officer released the *Federal Cloud Computing Strategy*.⁵ This strategy outlines a three-phase framework for selecting, provisioning, and managing cloud systems.

- Selecting Phase – consists of assessing potential information technology systems for cloud migration by two factors: 1) business value and 2) cloud readiness.
- Provisioning Phase – consists of aggregating demand at the departmental level to pool purchasing power; integrating services into a wider information technology portfolio; generating contracts for cloud services with explicit service level agreements that include, but are not limited to, security, continuity of operations, and service quality; and ensuring that legacy systems are decommissioned to realize the full potential of the new cloud solution.
- Managing Phase – consists of beginning to manage services rather than assets. This process consists of actively monitoring the service level agreements in place as well as regular re-evaluation of the service provider to ensure that the vendor is meeting all expectations set by the contracts and agreements in place.

The Internal Revenue Manual (IRM)⁶ states that the agency should provide a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services in line with the U.S. Chief Information Officer’s cloud first policy.

The National Institute of Standards and Technology⁷ guidance states that organizations must develop and maintain an inventory of its information systems. The inventory should accurately

⁵ The White House, U.S. Chief Information Officer Vivek Kundra, *Federal Cloud Computing Strategy* (Feb. 2011).

⁶ IRM 10.8.24 (May 2, 2016).

⁷ National Institute of Standards and Technology Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

reflect the cloud service and, at a minimum, include system association and system owner, and be reviewed and updated on a routine basis. The National Institute of Standards and Technology also recommends that an organization employ automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information systems. The IRM⁸ states that the IRS shall develop and maintain an inventory of information systems.

We spoke multiple times with officials in the Information Technology organization's Enterprise Operations and Enterprise Services organizations to discuss the IRS's progress in defining and developing an enterprise-wide cloud strategy. In July 2016, the IRS created an Integrated Planning Team with an overall goal of developing an enterprise-wide cloud strategy for implementation within the IRS. The Integrated Planning Team's mission is to help the IRS define a "cloud" and to layout some specific guidance to assist in the selection and deployment of cloud service within the IRS. At the end of our fieldwork, the Integrated Planning Team had not yet formulated an IRS definition for a cloud. As part of our discussions, the Integrated Planning Team shared some of the specifics related to its work to develop an IRS enterprise-wide cloud strategy:

- Meetings have been informal.
- There is no established implementation date.
- It should apply to all enterprise-wide cloud technologies.
- It should be used when cloud service opportunities exist.

To evaluate service providers and compare their services to traditional information technology, the IRS plans to review technical requirements, management requirements, operational requirements, monitoring requirements, Federal Risk and Authorization Management Program (FedRAMP) certification (vendors), and how to manage multiple cloud providers.

We requested a copy of the IRS's cloud inventory at the beginning of the audit and followed up several times throughout the course of the audit. Multiple Information Technology organization functions stated that an inventory of cloud services did not exist. Near the end of our fieldwork, officials from the Cybersecurity organization provided an inventory spreadsheet consisting of two columns. We interviewed Cybersecurity organization officials responsible for developing and maintaining the inventory and were told that the spreadsheet is manually updated when Change Management Requests are submitted. The change request is the primary means by which the Cybersecurity organization is notified when systems need to be added to the inventory. Cloud services are added to the inventory in chronological order once Cybersecurity organization officials are made aware of the system. The only data documented for each system are the name of the system and the associated cloud service provider. The inventory does not distinguish between deployed systems, systems in development, system ownership, or other informative

⁸ IRM 10.8.1 (Dec. 23, 2013).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

details. We determined that reliance on change management requests to manually maintain a list of IRS cloud systems, either planned or deployed, is insufficient for an inventory of cloud systems.

Although the IRS has taken steps to develop an enterprise-wide cloud strategy, it remains in the early stages of defining an official enterprise-wide policy for the cloud strategy/framework. The IRS stated that there is no current timetable for adoption and implementation of the enterprise-wide cloud strategy.

The U.S. Chief Information Officer's cloud guidance was issued in the Calendar Year 2010 and 2011 timeframe; however, the IRS did not prioritize the creation of a project team to develop an enterprise-wide cloud strategy until Fiscal Year 2016. Similarly, the IRS did not begin its inventory of cloud services until November 2015.

Without a documented strategy for the selection, management, and inventory of cloud services, there are multiple risks which include: 1) a repeat of the Form 990, *Return of Organization Exempt From Income Tax*, project discussed in the next finding in which information technology services were acquired outside of and without the support of the IRS Information Technology organization; 2) deployed cloud services will not meet the business and technical needs for a production system; 3) the inability of the IRS to effectively provision or manage selected services once implemented; 4) potential wasted resources because the IRS could deploy multiple, duplicative, and overlapping systems with no coordination; and 5) the inventory list of all IRS cloud services may be inaccurate. Without an accurate inventory, the IRS does not know what it has deployed and therefore what it should be protecting.

Recommendations

The Chief Information Officer should:

Recommendation 1: Prioritize and complete an enterprise-wide cloud strategy that is in alignment with Federal guidance.

Management's Response: The IRS agreed with this recommendation. The IRS plans to continue its ongoing efforts to formulate, socialize, and publish an enterprise-wide cloud strategy. This strategy artifact will identify and formalize necessary people, process, technology, and methodology changes that the IRS plans to implement which will enable it to strategically pursue, procure, deploy, and manage cloud services within the IRS.

Recommendation 2: Ensure that the process of managing the IRS's cloud inventory is formalized using automated methods and updated on a periodic and ongoing basis as part of the enterprise-wide cloud strategy.

Management's Response: The IRS agreed with this recommendation in part. As part of the IRS's cloud strategy effort, it plans to identify and recommend formalization of specific



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

cloud inventory management processes. It plans to identify and recommend specific changes in project initiation processes that have a cloud impact, to be incorporated where appropriate, with its enterprise life cycle process. However, and especially in light of the IRS's limited resources, the IRS does not believe an "automated solution" is either necessary or can be cost-effectively supported.

Office of Audit Comment: While we acknowledge the budget limitations, some automated process should be implemented per National Institute Standards and Technology guidance to ensure that the Information Technology organization is notified about cloud procurements and other related inventory changes.

**The Internal Revenue Service Did Not Follow Federal and Agency
Cloud Service Guidelines for the Form 990 Cloud Project**

A December 2011 Office of Management and Budget memorandum⁹ mandated that agencies use the FedRAMP to conduct risk assessments, perform security authorizations, and grant Authorities to Operate for all Executive department or agency use of cloud services.

The IRM¹⁰ defines enterprise-wide roles and responsibilities related to information and computer security. Specifically, it states that the agency head ensures that each information system is assigned an authorizing official and that no information systems are operated in production environments without an assigned authorizing official.

Additionally, the IRM¹¹ specifies that FedRAMP security requirements are to be followed for information technology projects that contract or employ cloud service providers and cloud services or applications. It also states that the IRS shall designate an authorizing official for each cloud computing service. According to FedRAMP guidance, authorizing officials monitor both the Plan of Action and Milestones and any major significant changes and reporting artifacts (such as vulnerability scan reports) associated with the cloud service. According to FedRAMP guidance, authorizing officials use this information so that risk-based decisions can be made about ongoing authorizations.

In January 2015, a Federal judge in California ruled against the IRS in a Freedom of Information Act¹² case, thus requiring the IRS to provide certain Form 990 information publicly accessible in the same machine-readable format as Modernized E-file data.¹³ The Form 990 is required for

⁹ Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 2011).

¹⁰ IRM 10.8.2 (Sept. 30, 2016).

¹¹ IRM 10.8.24 (May 2, 2016).

¹² 5 United States Code § 552 (2013).

¹³ *Public.Resource.Org v. United States IRS*, 2015, 2015 U.S. Dist. LEXIS 175943 (N.D. Cal. Nov. 20, 2015).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

tax-exempt organizations, nonexempt charitable trusts, and Section 527 political organizations to ensure that they comply with the tax law.¹⁴

Subsequently, the Commissioner, Tax Exempt and Government Entities Division, was tasked to create a process that would deliver this return information proactively, while attempting to automate the redaction process. The IRS initiated the Form 990 cloud service project in November 2014, and the innovation phase (design, development, testing, and production) lasted 20 months. In June 2016, the publicly accessible Form 990 data were put into production with an initial data set of 1.4 million records.

FedRAMP granted Amazon Web Services GovCloud (US) a Provisional Authorization to Operate in May 2016. However, if an agency chooses to use the Amazon Web Services GovCloud (US), it must create its own Authority to Operate letter to show that it is accepting the security risk associated with the cloud service. The FedRAMP program cannot make decisions for the IRS or accept risk on its behalf. Additionally, agencies are directed to provide a copy of the Authority to Operate letter to the FedRAMP program.

The IRS did not appoint an authorizing official or generate an agency-specific Authority to Operate letter for the Form 990 cloud service. As a result of this oversight, the IRS did not make a proper risk-based decision prior to placing this system into production. Without an assigned authorizing official and agency-specific Authority to Operate letter, the IRS cannot ensure that the Form 990 cloud service operates with an acceptable level of risk to agency operations, agency assets, other organizations, and the taxpayer.

The current Form 990 cloud service user agreement does not contain any mandated Federal risk and authorization management program clauses or service level agreements

A December 2011 Office of Management and Budget memorandum¹⁵ requires Federal agencies to ensure that FedRAMP requirements are met through contractual provisions. To assist agencies in meeting this requirement, the FedRAMP Program Management Office provides standard template contract language as well as template contract clauses covering all FedRAMP requirements. In February 2012, the U.S. Chief Information Officer Council and the Chief Acquisition Officers Council, in coordination with the Federal Cloud Compliance Committee, published *Creating Effective Cloud Computing Contracts for the Federal Government Best Practices for Acquiring IT as a Service*.¹⁶ This document provides Federal agencies more

¹⁴ Returns by Exempt Organizations, Consolidated Appropriations Act 2016, Pub. L. No. 114-113, 129 Stat. 3118 (2015).

¹⁵ Office of Management and Budget, *Security Authorization of Information Systems in Cloud Computing Environments* (Dec. 2011).

¹⁶ U.S. Chief Information Officer Council, Chief Acquisition Officers Council, and Federal Cloud Compliance Committee, *Creating Effective Cloud Computing Contracts for the Federal Government, Best Practices for Acquiring IT as a Service* (Feb. 2012).



The Internal Revenue Service Does Not Have a Cloud Strategy and Did Not Adhere to Federal Policy When Deploying a Cloud Service

specific guidance to effectively implement the cloud first policy and move forward with the Federal Cloud Computing Strategy. According to this guidance, service level agreements between a cloud service provider and a Federal agency are necessary in order to define acceptable service levels to be provided by the cloud service provider to its customers in measurable terms. The ability of a cloud service provider to perform at acceptable levels is consistent among service level agreements, but the definition, measurement, and enforcement of this performance varies widely among cloud service providers. Federal agencies should ensure that cloud service provider performance is clearly specified in all service level agreements, and that all such agreements are fully incorporated, either by full text or by reference, into the cloud service provider contract.

Based on case study analysis and guidance issued by the Office of Management and Budget, the Government Accountability Office¹⁷ compiled a list of 10 best practices for Federal agencies to incorporate into a contract for cloud computing services. Figure 1 shows the key practices organized by the management areas of roles and responsibilities, performance measures, security, and consequences.

Figure 1: Key Practices for a Cloud Computing Service Level Agreement

Roles and responsibilities	
1.	Specify roles and responsibilities of all parties with respect to the service level agreement, and at a minimum, include agency and cloud providers.
2.	Define key terms, such as dates and performance.
Performance measures	
3.	Define clear measures for performance by the contractor. Include which party is responsible for measuring performance. Examples of such measures would include: <ul style="list-style-type: none">- Level of service, <i>e.g.</i>, service availability—duration the service is to be available to the agency.- Capacity and capability of cloud service, <i>e.g.</i>, maximum number of users that can access the cloud at one time and ability of provider to expand services to more users.- Response time, <i>e.g.</i>, how quickly cloud service provider systems process a transaction entered by the customer, response time for responding to service outages.
4.	Specify how and when the agency has access to its own data and networks. This includes how data and networks are to be managed and maintained throughout the duration of the service level agreement and transitioned back to the agency in case of exit/termination of service.

¹⁷ Government Accountability Office, GAO-16-325, *CLOUD COMPUTING: Agencies Need to Incorporate Key Practices to Ensure Effective Performance* (Apr. 7, 2016).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

5. Specify the following service management requirements: <ul style="list-style-type: none">- How the cloud service provider will monitor performance and report results to the agency.- When and how the agency, via an audit, is to confirm performance of the cloud service provider.
6. Provide for disaster recovery and continuity of operations planning and testing, including how and when the cloud service provider is to report such failures and outages to the agency. In addition, how the provider will remediate such situations and mitigate the risks of such problems recurring.
7. Describe any applicable exception criteria when the cloud service provider's performance measures do not apply, <i>e.g.</i> , during scheduled maintenance or updates.
Security
8. Specify metrics the cloud provider must meet in order to show it is meeting the agency's security performance requirements for protecting data, <i>e.g.</i> , clearly define who has access to the data and the protections in place to protect the agency's data.
9. Specify performance requirements and attributes defining how and when the cloud service provider is to notify the agency when security requirements are not being met, <i>e.g.</i> , when there is a data breach.
Consequences
10. Specify a range of enforceable consequences, such as penalties, for noncompliance with service level agreement performance measures.

Source: Government Accountability Office.¹⁸

The IRS signed a user agreement with Amazon Web Services in May 2016 to host the IRS's Form 990 data via a public cloud service. The current user agreement between the IRS and Amazon Web Services is executed at no cost to the Government, although the IRS did pay a total of approximately \$18 from January through March 2016 for the use of Application Program Interface tools. The current user agreement does not contain any service level agreements or any cloud contract best practices, which the Federal Chief Information Officer Council, Chief Acquisition Officers Council, and Federal Cloud Compliance Committee designated as key factors in ensuring the success of cloud services.

In part as a result of the IRS's lack of an enterprise-wide cloud strategy, the Tax Exempt and Government Entities Division entered into an agreement to utilize a public cloud service with limited involvement from the IRS Information Technology organization. In October 2015, the Tax Exempt and Government Entities Division had discussions with the Associate Chief Information Officer for Enterprise Services regarding the Form 990 project. However, the Tax Exempt and Government Entities Division was not instructed to appoint an authorizing official, generate an agency Authority to Operate letter, or ensure that the cloud service complied with

¹⁸ Government Accountability Office, *GAO-16-325, CLOUD COMPUTING: Agencies Need to Incorporate Key Practices to Ensure Effective Performance* (Apr. 7, 2016).



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

FedRAMP requirements. By not adhering to Federal guidelines regarding cloud implementation, the IRS risks Form 990 data accuracy and availability issues due to the lack of clearly defined roles and responsibilities for the cloud service provider in measurable terms. Additionally, the IRS did not incorporate any service level agreements into the current user agreement with Amazon Web Services. At a minimum, the IRS should ensure that the service level agreement contains clearly defined terms, definitions, and performance parameters, and also defines who is responsible for measuring service level agreement performance.

Recommendations

The Chief Information Officer should:

Recommendation 3: Designate an authorizing official, complete the required FedRAMP Security Assessment Report, and issue an agency-specific Authority to Operate letter for the Form 990 cloud service.

Management's Response: The IRS agreed with this recommendation. The IRS plans to designate an authorizing official for the Form 990 Cloud Service. The Cybersecurity organization plans to assess the 990 Cloud Service solution and applicable FedRAMP security documentation and ensure that a Security Assessment Report and an Authority to Operate letter are issued.

Recommendation 4: Ensure that the Form 990 cloud service includes a service level agreement that defines acceptable service levels to be provided by the cloud service provider in measurable terms.

Management's Response: The IRS disagreed with this recommendation. The IRS stated that under applicable law, the Form 990 data are publicly available; the IRS may disclose them directly and may post them on the publicly accessible site. Amazon Web Services is allowing free access to the electronically filed Form 990 data from a repository for the convenience of the public, but the IRS is neither procuring nor acquiring any services or products from Amazon Web Services. Pursuant to written legal advice of counsel, the IRS ensured that the disclosure, procurement, and information security terms of the Amazon Web Services arrangement were acceptable. Consequently, the IRS and Amazon Web Services agreed to the current Terms of Use. Beyond these terms, it is unclear that a service level agreement would be appropriate for the free access arrangement, for which no payment or procurement actions are authorized.

Office of Audit Comment: Service level agreements between a cloud service provider and a Federal agency are necessary in order to define acceptable service levels to be provided by the cloud service provider to its customers in measurable terms. However, the IRS did not enter into a service level agreement and its approach for obtaining the cloud service has potential drawbacks. For example, according to the



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Amazon Web Services Customer Agreement, Amazon may terminate services to the IRS with only a 30-day notice. This could leave the IRS without a solution to provide Form 990 data in machine-readable format—as required per the U.S. District Court ruling—with little notice. Without a defined service level agreement in place, the IRS risks not being able to provide Form 990 data as required while a new solution is developed.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to review the IRS cloud strategy and how it has been implemented. To accomplish our objective, we:

- I. Determined the status of the IRS enterprise-wide cloud strategy.
 - A. Interviewed IRS officials involved with the strategy's development.
 - B. Reviewed IRS charter and working group documentation.
 - C. Identified and evaluated agency goals for cloud computing.
 - D. Evaluated possible causes for any implementation delays.
 - E. Conducted research and performed interviews to identify IRS cloud service implementations.
- II. Determined whether the Form 990 cloud service with Amazon Web Services complied with Federal guidelines.
 - A. Reviewed the process the IRS followed to develop a business value for cloud readiness for the Form 990 cloud service.
 - B. Reviewed the security controls, procedures, policies, contracts, and service level agreements in place to track the performance of the cloud service provider and manage the risks of Federal program and personal data stored on cloud systems.

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: National Institute of Standards and Technology Special Publications requirements for security and privacy of Federal information systems and cloud computing, and IRM policies related to cloud computing and security. We evaluated these controls by interviewing IRS personnel and reviewing relevant documentation provided by the IRS to gain an understanding of the policies and procedures related to the IRS enterprise-wide cloud strategy.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
John L. Ledford, Director
Jena Whitley, Audit Manager
Nicholas Reyes, Lead Auditor
Michael Curtis, Senior Auditor



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Director, Office of Audit Coordination



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Appendix IV

Glossary of Terms

Term	Definition
Amazon Web Services GovCloud (US)	An isolated Amazon Web Services region designed to host sensitive data and regulated workloads in the cloud, helping customers support their U.S. Government compliance requirements, including FedRAMP.
Application Program Interface	A set of routines, protocols and tools referred to as “building blocks” used in business application software development.
Authority to Operate	After completing a security assessment, the head of an agency (or their designee) can authorize the system for use, or grant an Authority to Operate according to a risk-based framework that analyzes how a vendor has implemented the security controls within its information technology environment.
Authorizing Official	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Change Management Requests	The transition of a changed or new product from development/acquisition through deployment of any IRS technology asset (<i>e.g.</i> , Production, Development, Test, Disaster Recovery, <i>etc.</i>) with minimum disruption to the users of IRS information technology.
Cloud First Policy	As part of the U.S. Chief Information Officer’s plan to reform Federal Information Technology Management, all Federal agencies were required to shift to a “cloud first” policy. When agencies are evaluating options for new information technology deployments, the Office of Management and Budget requires that agencies default to cloud solutions whenever a secure, reliable, cost-effective cloud option exists.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Term	Definition
Community Cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns, <i>e.g.</i> , mission, security requirements, policy, and compliance considerations. It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Federal Risk and Authorization Management Program	A Governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30. The fiscal year is designated by the calendar year in which it ends. Congress passes appropriations legislation to fund the Government for every fiscal year.
Hybrid Cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability, <i>e.g.</i> , cloud bursting for load balancing between clouds.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.
Infrastructure As a Service	The capability to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components, <i>e.g.</i> , host firewalls.
Modernized E-file	An IRS program that receives and processes tax returns in an Internet environment.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Term	Definition
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 Government agency operations and assets.
Plan of Action and Milestones	A document that identifies tasks 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.
Platform As a Service	The capability to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers, <i>e.g.</i> , business units. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.
Provisional Authorization to Operate	An initial approval of a cloud service provider authorization package by the FedRAMP Joint Authorization Board that an Executive department or agency can leverage to grant a security authorization and accompanying authority to operate for the acquisition and use of the cloud service within their agency.
Public Cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or Government organization, or some combination of them. It exists on the premises of the cloud provider.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Term	Definition
Security Authorizations	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed upon set of security controls.
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, <i>e.g.</i> , 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.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

Appendix V

Management's Response to the Draft Report

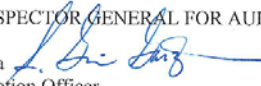


CHIEF INFORMATION OFFICER

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

JUN 13 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza 
Chief Information Officer

SUBJECT: Draft Audit Report - The Internal Revenue Service Does
Not Have A Cloud Strategy And Did Not Adhere To
Federal Policy When Deploying A Cloud Service
(201620021)

Thank you for the opportunity to review your draft audit report and to discuss earlier draft report observations with the audit team.

IRS Information Technology (IT) is very aware of the "cloud first" strategy and framework released by the U.S. Chief Information Officer (CIO) and has taken steps to strategically adopt cloud services. As a primary example, in 2013 the IRS successfully implemented the Integrated Enterprise Portal (IEP) program. The IEP enables one-stop, web-based services for internal and external users through a fully scalable and secure managed private cloud capability. The IRS won the 2014 Government Computer News IT Award for Achievement in recognition of this significant accomplishment.

Developing an enterprise-wide cloud strategy is of critical importance to the Internal Revenue Service (IRS). We have established a cross-functional team to formulate, socialize and publish an enterprise-wide strategy with a planned delivery date of October 2017. Additionally, we have documented policy that defines security controls for IRS Cloud Computing Systems.¹

This report discusses a cloud service used by the Tax-Exempt/Government Entities (TE/GE) Business Operating Division to allow access to the public data from Form 990, *Return of Organization Exempt from Income Tax*. We agree that IRS IT must be involved in Business Operating Division procurement and implementation of cloud services. IRS IT and the TE/GE organization will designate an Authorizing Official for TE/GE's Form 990 public cloud service to ensure a FedRAMP Security Assessment Report is completed, and if appropriate, an Authority to Operate document is issued. Additionally, we will formalize the process for managing the IRS cloud inventory as part of the overarching cloud strategy.

¹ Internal Revenue Manual (IRM) 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* effective May 2, 2016.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

The issuance of Service Level Agreements (SLA) is project-specific. Pursuant to written legal advice of counsel, IRS ensured that disclosure, procurement, and information security terms of the Amazon Web Service arrangement for the Form 990 project were acceptable. As such, we disagree that a SLA is required in this case.

We are committed to continuously improving our information technology strategies, systems and processes.

The continued support, assistance and guidance your team provides is very valuable to us in this regard. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Carmelita White at (240) 613-2191.

Attachment



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

The Internal Revenue Service Does Not Have A Cloud Strategy And Did Not Adhere To Federal Policy When Deploying A Cloud Service (Audit # 201620021)

RECOMMENDATION #1: Prioritize and complete an enterprise-wide cloud strategy that is in alignment with Federal guidance.

CORRECTIVE ACTION #1: The IRS agrees with this recommendation. We will continue our ongoing effort to formulate, socialize and publish an Enterprise-wide Cloud Strategy. This strategy artifact will identify and formalize necessary people, process, technology and methodology changes that we will seek to implement which will enable us to strategically pursue, procure, deploy and manage Cloud services within the IRS.

IMPLEMENTATION DATE: Our target date for formal publication of the IRS Cloud Strategy is October 1, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion.

RECOMMENDATION #2: Ensure that the process of managing the IRS's cloud inventory is formalized using automated methods and updated on a periodic and ongoing basis as part of the enterprise-wide cloud strategy.

CORRECTIVE ACTION #2: The IRS agrees with this recommendation in part. As part of our Cloud Strategy effort, we will identify and recommend formalization of specific Cloud inventory management processes. We will identify and recommend specific changes in project initiation processes that have a Cloud impact, to be incorporated where appropriate, with our enterprise life cycle (ELC) process. However, and especially in light of our limited resources, we do not believe an "automated solution" is either necessary or can be supported cost effectively.

IMPLEMENTATION DATE: Our target date for formal publication of the IRS cloud Strategy is October 1, 2017. Specific implementation timelines of ensuing processes will be identified as part of the strategy.

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion.



*The Internal Revenue Service Does Not Have
a Cloud Strategy and Did Not Adhere to Federal Policy
When Deploying a Cloud Service*

The Internal Revenue Service Does Not Have A Cloud Strategy And Did Not Adhere To Federal Policy When Deploying A Cloud Service (Audit # 201620021)

RECOMMENDATION #3: Designate an authorizing official, complete the required FedRAMP Security Assessment Report, and issue an agency specific Authority to Operate letter for the Form 990 cloud service.

CORRECTIVE ACTION #3: The IRS agrees with this recommendation. We will designate an Authorizing Official (AO) for the Form 990 Cloud Service. Cybersecurity will assess the 990 Cloud Service solution and applicable FedRAMP security documentation and ensure a Security Assessment Report and Authority to Operate are issued.

IMPLEMENTATION DATE: August 15, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES). These Corrective Actions are monitored on a monthly basis until completion.

RECOMMENDATION #4: Ensure that the Form 990 cloud service includes a service level agreement that defines acceptable service levels to be provided by the cloud service provider in measurable terms.

CORRECTIVE ACTION #4: The IRS disagrees with this recommendation. Under applicable law, the Form 990 data are publicly available; IRS may disclose them directly and may post them on the publicly-accessible site. Amazon Web Services (AWS) is allowing free access to the electronically-filed Form 990 data from a repository for the convenience of the public, but IRS is neither procuring nor acquiring any services or products from AWS. Pursuant to written legal advice of counsel, IRS ensured that disclosure, procurement, and information security terms of the AWS arrangement were acceptable. Consequently, IRS and AWS agreed to the current Terms of Use. Beyond these terms, it is unclear that a service level agreement would be appropriate for the free access arrangement, for which no payment or procurement actions are authorized.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL: N/A

CORRECTIVE ACTION MONITORING PLAN: N/A