Internal Revenue Service (IRS) Publication 1075 Compliance in AWS

February 2018

This paper has been archived.

For the latest version of this paper, see https://docs.aws.amazon.com/whitepapers/latest/internal-revenue-service-publication-1075-compliance-in-aws/welcome.html

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

The Internal Revenue Service Publication 1075 (IRS 1075) compliance whitepaper has been designed to guide Customers that receive FTI on their compliance responsibilities as part of the "Shared Responsibility" while using Amazon Web Services (AWS). The document is to be used by Customers that are subject to the IRS 1075 requirements governing use and access to FTI.

IRS 1075 requires the use of specific security controls covered under FedRAMP control baselines. AWS is audited for relevant IRS 1075 controls under The Federal Risk and Authorization Management Program (FedRAMP), a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

AWS offers the following FedRAMP compliant systems that: meet applicable requirements and authorizations, address the FedRAMP security controls (based on NIST SP 800-53 rev 4), use the required FedRAMP templates for security packages posted in the secure FedRAMP repository, have been assessed by an accredited independent 3rd Party Assessment Organization (3PAO), and comply with the continuous monitoring requirements of FedRAMP:

- AWS GovCloud (US), has been granted a Joint Authorization Board Provisional Authority-To-Operate (JAB P-ATO) and multiple Agency Authorizations (A-ATO) for the "high" impact level. For a list of authorizing agencies who have issued an ATO on AWS GovCloud (US), please visit FedRAMP Compliant Systems.
- AWS US East-West, has been granted multiple Agency ATOs for the "moderate" impact level. For a list of authorizing agencies who have issued an ATO on AWS US East-West please visit FedRAMP Compliant Systems.

Customers may require specific configurations, connectivity, and architecture when using AWS in support of an IRS 1075-compliant environment. This paper provides an overview of AWS service capabilities, including security services and tools that parties working with FTI should implement when architecting to meet IRS 1075 requirements under the "Shared Responsibility" model.

IRS 1075 Background

The Internal Revenue Service Publication 1075 (IRS 1075) provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient agencies, agents, or contractors (Customers) adequately protect the confidentiality of Federal Tax Information (FTI). IRS 1075 provides guidance for US government agencies and their agents that access FTI to ensure that they use policies, practices, and controls to protect FTI confidentiality.

The IRS publication contains the managerial, operational, and technical security controls that must be implemented as a condition of receipt of FTI. The guidelines outlined apply to all FTI, no matter the amount or the media in which it is recorded. As a condition of receiving FTI, the receiving party must show, to the satisfaction of the IRS, the ability to protect the confidentiality of that information. Safeguards must be implemented to prevent unauthorized access and use. The IRS may require formal agreements that specify, among other things, how the information will be protected. A receiving party must ensure its safeguards will be ready for immediate implementation upon receipt of FTI.

Additionally, as Customers receiving FTI look to reduce costs and improve operations, they can look to cloud services (like AWS) to help streamline their processes and applications. This is contemplated by the IRS Office of Safeguards Technical Assistance Memorandum dated June 2013, which outlines requirements when working with FTI in a cloud computing environment. The IRS memorandum outlines the use of NIST guidance, FedRAMP control baselines, industry best practices, and the Internal Revenue Service (IRS) Publication 1075 requirements. Referenced: Protecting FTI in a Cloud Computing Environment.

Introduction

To foster a tax system based on voluntary compliance, the public must maintain a high degree of confidence that the personal and financial information furnished to the Internal Revenue Service (IRS) is protected against unauthorized use, inspection, or disclosure. The IRS must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of the public trust.

The IRS 1075 publication provides guidance to ensure the policies, practices, controls, and safeguards employed by recipient Customers adequately protect the confidentiality of FTI. Enterprise security policies address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance to implement all applicable security controls.

AWS maintains two FedRAMP authorizations –the AWS GovCloud (US) region (FedRAMP high) and the AWS US East/West regions (FedRAMP moderate). With these authorizations, customers inherit comprehensive security and compliance controls, and strengthen their own compliance and certification programs. As the IRS safeguard memo outlines, “cloud computing may offer promise as an alternative to traditional data center models.” By utilizing AWS cloud services, agencies may be able to reduce hardware and personnel costs by eliminating redundant operations and consolidating resources. Customers can leverage AWS’s FedRAMP authorizations to comply with IRS requirements for storing and protecting FTI in the cloud. Individual applications will be evaluated by the IRS Office of Safeguards as part of the cloud computing notification. See Section: IRS 1075 Mandatory Requirements for FTI in a Cloud Environment.

AWS Management Environment

AWS’s world-class, highly secure data centers utilize state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least-privilege basis. Environmental systems are designed to minimize the impact of disruptions to operations, and multiple geographic regions and Availability Zones allow you to remain resilient in the face of most failure modes, including natural disasters or system failures.

Physical and Environmental Security

AWS’s data centers are state-of-the-art, utilizing innovative architectural and engineering approaches. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means.

Secure Network Architecture

Network devices, including firewall and other boundary devices, are in place to monitor and control communications at the external boundary of the network, and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

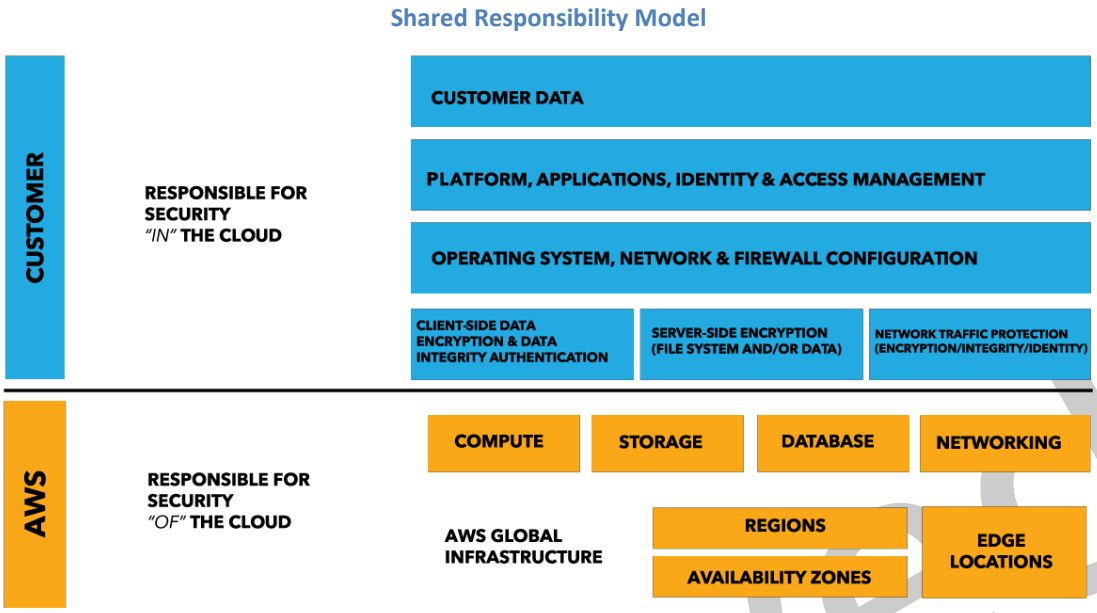
Network Monitoring and Protection

AWS utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. AWS monitoring tools are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. The tools have the ability to set custom performance metrics thresholds for unusual activity.

AWS Shared Responsibility Model

As with any hyperscale CSP, utilizing AWS creates a shared responsibility model for the operation and management of security controls. This shared model can help relieve a layer of operational burden as both AWS and you operate, manage, and control components of information security controls. In terms of information security and compliance in cloud computing, there is a subtle but very important distinction in understanding and evaluating compliance of the cloud solution and understanding and evaluating your compliance in your cloud solution. “Security and Compliance OF the cloud” pertains to the security programs and measures which the Cloud Service Provider (i.e. AWS) implements within the cloud infrastructure; “Security and Compliance IN the cloud” relates to the implementation of

security controls associated with Customer workloads running on top of the AWS infrastructure.



Security & Compliance OF the Cloud

Hyperscale cloud providers have readily available services and supporting architectures to offer both defense in depth and defense in breadth capabilities. This is due to security mechanisms being intrinsic to service design and operation. In order to manage risk and security within the cloud, a variety of processes and guidelines have been created to differentiate between the security of a cloud service provider and the responsibilities of a customer consuming the cloud services. One of the primary concepts that have emerged is the increased understanding and documentation of shared, inherited or dual (AWS & Customer) security controls in a cloud environment. A common question for AWS is: **"how does leveraging AWS make my security and compliance activities easier?"** This question can be answered by considering the security controls that a customer inherits through its use of the AWS services in two general ways: first, reviewing compliance of the AWS Infrastructure gives an idea of "Security & Compliance OF the cloud"; and second, reviewing the security of workloads running on top of the AWS infrastructure gives an idea of "Security & Compliance **IN** the cloud".

AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. Customers running workloads in the AWS infrastructure depend on AWS for a number of security controls. AWS has several whitepapers that provide additional information to assist Customers with integrating AWS into their existing security frameworks and to help design and execute security assessments of an organization's use of AWS. Reference: AWS Risk & Compliance Whitepaper.

Mandatory Requirements for FTI in a Cloud Environment

To utilize a cloud computing model to receive, transmit, store, or process FTI, the receiving party must be in compliance with all IRS Publication 1075 requirements. The following mandatory requirements must be met before a Customer can introduce FTI to a cloud environment:

1. **Notification Requirement.** The agency must notify the IRS Office of Safeguards using their required form at least 45 days prior to transmitting FTI into a cloud environment. The version of the form as of the date of this White Paper can be found at: Cloud Computing Notification Form

2. **Data Isolation.** Software, data, and services that receive, transmit, process, or store FTI must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.

   How AWS supports Data Isolation for IRS 1075 workloads:

   a. **AWS Private Networking** - Network isolation allows agencies to maintain a secure environment and consistent user experience. By default, AWS creates your instances in a virtual private cloud (VPC) to provide customers with a logically isolated section of the AWS Cloud. Within the VPC, you maintain complete control over the network configuration.

   b. **AWS Private Compute** - Allows agencies to implement fine-grained access roles and groups for every workload. Depending on your needs, stages of isolation can be achieved with a username and password, a software-defined network, and dedicated instances for isolation at the hardware level.

   c. **AWS Private Storage** - Data security is fundamentally important for enterprise workloads, and AWS provides a wide assortment of private storage options. Amazon Simple Storage Service (Amazon S3) provides options for secure upload/download via SSL encrypted endpoints, as well as both client-side and server-side encryption options for data at rest.

3. **Service Level Agreements (SLA).** The agency must establish security policies and procedures based on IRS Publication 1075 for how FTI is stored, handled, and accessed inside the cloud through a legally binding contract or SLA with their third party cloud provider.

   How AWS supports SLA requirements of IRS 1075 workloads:

   AWS Data Privacy – At AWS, customer trust is our top priority. We deliver services to more than one million active customers, including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include

financial services providers, healthcare providers, and governmental agencies, all of which trust us with some of their most sensitive information.

We know customers care deeply about privacy and data security. That's why AWS gives customers ownership and control over their customer content by design through simple, but powerful tools that allow customers to determine where their customer content will be stored, secure their customer content in transit or at rest, and manage access to AWS services and resources for their users. We also implement responsible and sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer content. Reference: AWS Customer Agreement

Maintaining customer trust is an ongoing commitment; we strive to inform customers of the privacy and data security policies, practices, and technologies we've put in place. While the AWS Customer Agreement contains the full set of applicable terms and conditions, these commitments for ownership and control of customer content include:

- **Access:** Customers continue to fully own and manage access to their customer content and AWS services and resources. We provide an advanced set of access, encryption, and logging features to help Customers do this effectively (such as AWS CloudTrail). We do not take ownership, access, or use customer content for any purpose other than as required to provide and maintain the services.
- **Storage**: Customers choose the region(s) in which their customer content will be stored. We will not move or replicate customer content outside of the customer's chosen region(s) except as legally required and as necessary to maintain the AWS services and provide them to our customers and their end users.
- **Security:** Customers choose how their customer content is secured. We offer our customers strong encryption for customer content in transit or at rest, and we provide customers with the option to manage their own encryption keys (through AWS Key Management Service (KMS) or AWS CloudHSM).
- **Disclosure of customer content:** We do not disclose customer content unless we're required to do so to comply with the law. Where we're required to comply with law, we strive to provide notice to our customers (unless we're prohibited by law).
- **Security Assurance:** We have developed a Security Assurance Program using global privacy and data protection best practices in order to help customers establish, operate and leverage our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments and through Continuous Monitoring.

4. **Data Encryption in Transit.** FTI must be encrypted in transit within the cloud environment. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant, and operate utilizing FIPS 140-2 compliant modules.

   How AWS supports Data Encryption in Transit for IRS 1075 workloads:

   a. The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140-2 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL terminations in AWS GovCloud (US) operate using FIPS 140-2 validated hardware. AWS services in scope for FedRAMP meet IRS's requirement for FIPS 140-2 compliance for data in transit. AWS works with Customers to provide the information they need to help manage compliance when using the AWS GovCloud (US) or US East-West environments.

   b. AWS KMS has been validated by NIST for FIPS 140-2 compliance. (See NIST CMVP Cert #3009)

5. **Data Encryption at Rest.** FTI may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate FTI, encryption is a compensating control. All mechanisms used to encrypt FTI must be FIPS 140-2 compliant and operate utilizing FIPS 140-2 compliant modules.

   How AWS supports Data Encryption at Rest for IRS 1075 workloads:

   a. AWS KMS can be seamlessly integrated with several other AWS services. This integration means that you can easily use AWS KMS master encryption keys to encrypt the data you store when using the AWS services. You can use a default master key that is created for you automatically and usable only within the integrated service, or you can select a custom master key that you create in KMS and have permission to use.

   b. AWS KMS is designed so that no one has access to your master keys. The service is built on systems that are designed to protect your master keys with extensive hardening techniques such as never storing plaintext master keys on disk, not persisting them in memory, and limiting which systems can access hosts that use keys. All access to update software on the service is controlled by a multi-party access control that is audited and reviewed by an independent group within Amazon.

   c. To learn more about how AWS KMS works you can read the AWS Key Management Service whitepaper.

6. **Persistence of Data in Relieved Assets.** Storage devices where FTI has resided must be securely sanitized and/or destroyed using methods acceptable by National Security Agency/Central Security Service (NSA/CSS).

How AWS supports Data Sanitizing requirements for IRS 1075 workloads:

a. AWS uses the techniques detailed in NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. Additionally, customers are responsible for data sanitization of their data volumes and can run the same techniques outlined in DoD 5220.22-M.

7. **Risk Assessment.** The agency must conduct an annual assessment of the security controls in place on all information systems used for receiving, processing, storing, and transmitting FTI. For the annual assessment immediately prior to implementation of the cloud environment and each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment. The IRS Office of Safeguards will evaluate the risk assessment as part of the notification requirement in section 1, above.

How AWS supports Risk Assessment requirements for IRS 1075 workloads:

AWS customers should include their use of services within their annual risk assessment processes. Additionally, AWS's FedRAMP System Security Plan and supporting documentation can support agencies in monitoring AWS's risk posture.

8. Security Control Implementation. Customer defined security controls must be identified, documented, and implemented. The customer defined security controls, as implemented, must comply with Publication 1075 requirements.

How AWS supports Security Control Implementation requirements for IRS 1075 workloads:

a. Customers can leverage AWS's FedRAMP packages and authorizations in order to accelerate their Security Assessment and Authorization (SA&A) efforts. AWS provides customers with a package of security guidance and documentation to enhance their understanding of security and compliance while using AWS as a hosting solution.

b. For example, AWS provides an SSP template based upon NIST 800-53 Rev. 4, which is prepopulated with applicable control baselines. The controls within the template are prepopulated where applicable from AWS, shared between AWS and the customer, or fully the responsibility of the customer.

c. AWS customers can request access to the AWS FedRAMP security packages through their AWS Sales Account Manager.

d. AWS partners and prospective customers can also request access to the AWS FedRAMP Partner Package by contacting their AWS Sales Account Manager. The AWS FedRAMP Partner Package can also be retrieved directly from AWS Artifact in the AWS Management Console.

Creating an IRS 1075 Compliant Environment

AWS provides a number of ways for customers to comply with IRS 1075 requirements when using AWS services. Customers can architect an IRS 1075-compliant solution with FTI in the cloud using security features and functions, leveraging leading industry best practices. The following section provides a high-level overview of services and tools Customers should consider as part of their IRS 1075 implementation on AWS:

1. **Built-in firewalls** – Customers can control how accessible their instances are by configuring built-in firewall rules – from totally public to completely private, or somewhere in between.
2. **Authentication and Authorization** – There are two layers of authentication and authorization to consider in the AWS environment: IAM credentials and AWS customer controlled credentials. IAM provides authentication and authorization for direct access to AWS services by either using local IAM accounts, or integrating access controls with the AWS customer's corporate directory such as Active Directory.
3. **Guest Operating System** – Customers control virtual instances in Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Virtual Private Cloud (Amazon VPC). AWS customers have full administrative access and control over accounts, services, and applications.
    a. **Choosing an Operating System.** While AWS does provide images that can be used for deployment of host operating systems, AWS customers need to develop and implement system configuration and hardening standards to align with all applicable IRS 1075 requirements for their operating systems.
4. **Storage** – AWS provides various options for storage of information including Amazon Elastic Block Store (Amazon EBS), Amazon Simple Storage Service (Amazon S3), and Amazon Relational Database Service (Amazon RDS), to allow customers to make data easily accessible to their applications or for backup purposes. Storage of sensitive data in the various storage options should consider the technology and accessibility of the data and ensure that it meets IRS 1075 requirements for restricting direct inbound and outbound Internet access to the systems that contain sensitive data.
    a. For example, Amazon Simple Storage Service (Amazon S3) can be configured to require SSL as well as limit access to pre-defined IP Addresses to limit the accessibility of data from the Internet. Each storage option should be considered and designed to ensure that the use and storage of information is aligned with the relevant requirements.

5. **Private Subnets** – The AWS Virtual Private Cloud (VPC) service allows customers to add another layer of network security to their instances by creating private subnets and even adding an IPSec VPN tunnel between their home network and AWS VPC.
6. **Encrypted data storage** – Customers can have the data and objects they store in Amazon EBS, Amazon S3, Amazon Glacier, Amazon Redshift, and Oracle and SQL Server RDS encrypted automatically using Advanced Encryption Standard (AES) 256, a secure symmetric-key encryption standard using 256-bit encryption keys.
7. **Dedicated connection option** – The AWS Direct Connect service allows customers to establish a dedicated network connection from their premises to AWS. Using industry standard 802.1q VLANs, this dedicated connection can be partitioned into multiple logical connections to enable customers to access both public and private IP environments within the AWS cloud.
8. **Perfect Forward Secrecy** – For even greater communication privacy, several AWS services such as Elastic Load Balancer offer newer, stronger cipher suites. These cipher suites allow SSL/TLS clients to use Perfect Forward Secrecy, a technique that uses session keys that are ephemeral and not stored anywhere. This prevents the decoding of captured data, even if the secret long-term key itself is compromised.
9. **Security logs** – AWS CloudTrail provides logs of all user activity within a customer's AWS account. Customers can see who performed what actions on each of their AWS resources, and the AWS API call history produced by AWS CloudTrail enables security analysis, resource change tracking, and compliance auditing.
10. **Asset identification and configuration** – With the AWS Config service, Customers can immediately discover all of their AWS resources and view the configuration of each. Customers can receive notifications each time a configuration changes as well as dig into the configuration history to perform incident analysis.
11. **Centralized key management** – For customers who use encryption extensively and require strict control of their keys, the AWS Key Management Service provides a convenient management option for creating and administering the keys used to encrypt your data at rest.
12. **CloudHSM** – For customers who must use Hardware Security Module (HSM) appliances for cryptographic key storage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.

AWS Security Engineers and Solution Architects have developed whitepapers and operational checklists to help you select the best options for your needs and recommend security best practices, such as storing secret keys and passwords in a secure manner and rotating or changing them frequently.

While the IRS does not publish an official designation or certification for compliance with Pub 1075, AWS supports organizations to protect FTI managed in AWS by aligning our implementations of NIST 800-53 and FedRAMP security controls with the respective IRS Pub

1075 security requirements. AWS has worked closely with the IRS Office of Safeguards to align the AWS GovCloud (US) and AWS US East-West regions with Pub 1075 requirements for storing and processing FTI.

For more information on FedRAMP and AWS, please visit: https://aws.amazon.com/compliance/fedramp/

- For more information about IRS 1075, please visit: https://www.irs.gov/pub/irs-utl/p1075.pdf
- https://www.irs.gov/uac/Encryption-Requirements-of-IRS-Publication-1075

Appendix A – IRS Cloud Computing Notification Form

https://www.irs.gov/uac/additional-requirements-for-publication-1075

Introduction

April 2014 Update

To utilize a cloud computing model that receives processes, stores, or transmits FTI, the agency must notify the Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.

The IRS strongly recommends that an agency planning on implementing a cloud computing environment contact the Office of Safeguards at SafeguardReports@irs.gov to schedule a conference call to discuss the details of the planned cloud computing implementation. The agency should be prepared to discuss the requirements below with respect to their cloud computing environment.

The purpose of this document is to provide requirements for the information and documentation to include in the written notification to the IRS Office of Safeguards. This process will be used to assist the IRS in understanding and evaluating the state agencies cloud computing plans for compliance with IRS Publication 1075, and help ensure agencies build Publication 1075 security requirements into cloud computing environments.

How to Complete This Document

Agencies should review the security controls and compliance inquiries included below and provide their complete response in Part 1 of the form. This is a standalone form and it needs to stand on its own. Please ensure that all information is written out to address each control. **The IRS cannot accept any responses that reference other documents. This includes but is not limited to SSR, Agency Policy and Procedures, NIST, etc.** However this information may be transposed into this document.

All submissions should be sent to the IRS Safeguards mailbox (SafeguardReports@irs.gov) with the subject line: **Cloud Computing Notification.** The information requested through this document is not meant to be all-encompassing and the IRS may require additional information from the agency in order to evaluate the planned data warehouse implementation.

Document Workflow

The IRS will evaluate the agency's submission and complete Part 2 of the form. Upon submission of the table below, agencies may be contacted by the IRS Office of Safeguards for additional information or discussion based upon the specific facts provided about the cloud computing environment. Compliance with the Publication 1075 requirements for cloud computing environments will be routinely evaluated during the state agency's onsite Safeguard review.

Cloud Computing Notification Form – Part 1	
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
1	System and Services Acquisition	A. Will the cloud environment and associated systems be managed by the agency or another state agency (e.g., state IT department)? Or will it be handled by a vendor)? B. Identify where the equipment used in the cloud computing environment is hosted and physically resides.	Recipients of FTI are allowed to use a shared facility but only in a manner that does not allow access to FTI by employees, agents, representatives or contractors of other agencies using the shared facility.	[**Note:** Please be as detailed as possible in your responses.] Please place you response here using this format…

2	System and Services Acquisition (Contractors)	Certain FTI may not be included in a cloud environment where contractor access is prohibited by statute (e.g., Treasury Offset Program or access is prohibited by 6103 (l)(7). Please describe in detail what FTI will be in the cloud environment. Please describe how contractors and sub-contractors will be utilized in the cloud computing environment.	Access restrictions pursuant to the IRC authority by which the FTI is received continue to apply. For example, since human services agencies administering benefit eligibility programs may not allow contractor access to any FTI received, their data within the consolidated data center may not be accessed by any contractor of the data center. The agency must identify all contractors with access to FTI and the purpose for which access was granted. The agency must provide the name and address of the contractor.	
3	System and Services Acquisition (SLA or Contract Language)	A. Describe the contract or Service Level Agreement (SLA) in place with the cloud provider and identify whether it covers all of the requirements as listed in Publication 1075 under Section 5.5.2 and Exhibit 7.		

	Cloud Computing Notification Form – Part 1
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
		B. Provide a copy of the draft contract or SLA if available.		

4	System and Services Acquisition (Location of Operations)	A. Please provide a listing of where the cloud provider personnel and operations are located, including address. B. Certify that none of the cloud provider personnel or cloud provider operations and equipment or processing are located offshore.	FTI may not be accessed by contractor's employees located offshore or be included in contractor's information systems located off-shore. FTI may not be accessed by agency employees, agents, representatives or contractors located "offshore", outside of the United States or its territories. Further, FTI may not be received, stored, processed or disposed via information technology systems located off-shore.	All AWS GovCloud (US) and AWS US East-West systems are located within the continental United States.
5	System and Services Acquisition (Physical Security)	Please describe and provide a listing of the equipment that is used to receive, store, process, or transmit FTI and who owns the equipment.	Only agency-owned computers, media, and software will be used to receive, process, access, and store FTI. The agency must retain ownership and control, for all hardware, software, and endpoint equipment connecting to public communication networks, where these are resident at all alternate work sites.	All AWS GovCloud (US) and AWS US East-West systems are owned and operated by Amazon Web Services.
6	System and Information Integrity (Protection	A. Describe where the FTI data is stored in the cloud computing environment and how it will be	It is recommended that FTI be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures.	Within the AWS environment data is automatically distributed across physical facilities that are geographically separated within an AWS Region.

	Cloud Computing Notification Form – Part 1
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
	from Unauthorized Disclosure)	isolated from other customer's data. B. How is the information protected from inadvertent or unauthorized disclosure?		

7	System and Information Integrity (Incoming FTI and Encryption)	A. Describe how FTI is transitioned into the cloud environment. B. Who is responsible, how is it migrated in and who controls the authentication method that retrieves it electronically from the IRS?	The information system must protect the confidentiality of FTI during electronic transmission. When cryptography (encryption) is employed within the information system, the system must perform all cryptographic operations using Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules with approved modes of operation. Cryptographic data transmissions are ciphered and consequently unreadable until deciphered by the recipient.	
8	System and Information Integrity (Security Control Validation)	A. Describe how the agency for which the FTI is authorized, ensures that the cloud computing environment meets the physical and logical security requirements as outlined in Publication 1075. B. Describe what inspections are planned for the agency to verify security controls at the cloud provider, what the inspections will include, and how the results will be documented.	Agencies must ensure third-party providers of information systems, who are used to process, store and transmit federal tax information, employ security controls consistent with Safeguard computer security requirements. Another measure IRS requires is internal inspections by the recipient agency. The purpose is to ensure that adequate safeguard or security measures have been maintained.	AWS is assessed by a Third Party Assessor Organization to determine compliance of physical and logical security controls based on FedRAMP requirements (NIST 800-53 rev. 4 Security Controls). These controls align with IRS Pub 1075 requirements.

	Cloud Computing Notification Form – Part 1
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
9	System and Communications Protection	Describe how data is protected while in transit in the cloud environment and who is in control of the encryption keys.	All FTI data in transit must be encrypted when moving across a Wide Area Network (WAN) and within the agency's Local Area Network (LAN).	All FTI data in transit is encrypted when traversing the AWS FedRAMP boundary (i.e. traversing the WAN).

Cloud Computing Notification Form – Part 1	
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
10	Media Protection (Media Handling Procedures)	Describe what media (e.g., backup tapes or discs, external hard drives) in the cloud computing environment will contain FTI and how it will be sanitized and disposed of once no longer required.	The agency shall sanitize information system media prior to disposal or release for reuse.	AWS does not utilize backup tapes or discs within the datacenter. Additionally, external hard drives are prohibited from use. AWS sanitizes all forms of digital media, regardless if it is removable storage or non-removable storage. The media destruction devices used are on the NSA Evaluated Product List (EPL) and conform to approved sanitization methods as outlined in NIST SP 800-88 (clearing, purging, or destroying).

Cloud Computing Notification Form – Part 1	
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
11	Media Protection (Sanitization Notification)	Describe the policy and procedures implemented by the cloud provider to notify the agency upon of a storage device containing FTI that has failed, or situations where the data has been moved within the cloud environment or removed from the cloud environment.	Describe the amount and method of destruction for FTI (paper and/or electronic) disposed during the processing period.	AWS does not utilize backup tapes or discs within the datacenter. Additionally, external hard drives are prohibited from use. AWS sanitizes all forms of digital media, regardless if it is removable storage or non-removable storage. The media destruction devices used are on the NSA Evaluated Product List (EPL) and conform to approved sanitization methods as outlined in NIST SP 800-88 (clearing, purging, or destroying).

Cloud Computing Notification Form – Part 1	
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
12	Media Protection (Labeling and Commingling)	Describe the agency's methodology for labeling FTI prior to introducing it to the cloud environment and how commingled FTI will always be tracked and identified in the cloud environment. Describe the process to ensure FTI is labeled down to the data element level.	In situations where physical separation is impractical, the file should be clearly labeled to indicate that FTI is included and the file should be safeguarded. The information itself also will be clearly labeled.	

Cloud Computing Notification Form – Part 1	
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
13	Access Control	Describe how logical access controls are managed and granted in the cloud computing environment and who has control over the process and approvals.	Agencies must manage information system user accounts, including establishing, activating, changing, reviewing, disabling, and removing user accounts. The information system must enforce assigned authorizations for controlling system access and the flow of information within the system and between interconnected systems.	Logical access controls are managed directly by the agency through AWS IAM, as well as any on-premises identity management solutions.

14	Incident Response/ System and Service Acquisition	A. Describe what incident response policies, plans and procedures have been developed for the cloud environment. B. Have the notification requirements, including the specifics of reporting timeframes, information required to be reported, and the point of contact to which it should be reported been incorporated into the SLA/ contract?	Upon discovering a possible improper inspection or disclosure of FTI, including breaches and security incidents, by a federal employee, a state employee, or any other person, the individual making the observation or receiving information should contact the office of the appropriate Special Agent-in-Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS. The agency will contact TIGTA and the IRS immediately, but no later than 24-hours after identification of a possible issue involving FTI. The agency should not wait to conduct an internal investigation to determine if FTI was involved. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately.	AWS has developed an Incident Response plan that provides a high-level approach for how the incident response capability fits into the overall organization. AWS defines responder roles and responsibilities for the AWS security team, as well as roles for any affected service(s). AWS will contact affected customers in the case of confirmed security incidents.
15	Awareness and Training	Describe the training requirements for the cloud provider personnel who have access to systems that process, store, receive, or transmit FTI. Does the training content include information on the provisions of	Granting agency an employee or contractor access to FTI must be preceded by certifying that each employee or contractor understands the agency's security policy and procedures for safeguarding IRS information. Employees and	AWS Security maintains and provides basic security awareness training to all information system users supporting AWS.

		IRS Sections 7431, 7213, and 7213A?	contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, employees and contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information).	
16	Contingency Planning (Backup Frequency)	A. Describe how backups are handled, including what is backed up, to what is it backed up, according to what frequency, and where is it being stored (e.g. tapes, Storage Area Network (SAN)).	Agencies must conduct backups of user-level information, system-level information, and FTI and store such backups at a secure location.	AWS stores user-level information using the EBS and S3 storage services available within AWS. When data is stored in EBS or S3 redundant copies are automatically and synchronously created whenever the data is changed and the copies are validated to be identical to the original data.
17	Contingency Planning (Backup Media and Location)	B. List what medium backups are stored to and where those backups are located.	Agencies must identify alternate storage sites and initiate necessary agreements to permit the secure storage of information system and FTI backups.	AWS stores user-level information using the EBS and S3 storage services available within AWS. When data is stored in EBS or S3 redundant copies are automatically and synchronously created whenever the data is changed and the

	Cloud Computing Notification Form – Part 1
Date:	
Agency:	
POC Name:	
POC Title:	
POC Phone / Email:	[Please use this format (XXX) XXX-XXXX / E-Mail]
POC Site / Location:	
Site / Location FTI:	

#	Security Control	Compliance Inquiry	Requirements	Agency Response
				copies are validated to be identical to the original data.
18	Configuration Management (Customer Defined Security Controls)	Describe how the agency identifies, documents and implements customer defined security controls in compliance with Publication 1075 requirements.	Configuration management policy and procedures must be developed, documented, disseminated and updated as necessary to facilitate implementing configuration management security controls.	

19	Risk Assessment	Agencies are required to conduct a risk assessment (or update an existing risk assessment, if one exists) when migrating FTI to a cloud environment. Subsequently, the risk assessment must be reviewed annually to account for changes to the environment. This implementation and an evaluation of the associated risks should be part of the risk assessment.	Agencies must conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency regarding the use of FTI. The agency must update the risk assessment periodically or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.	

Publication 1075 Notification Requirements

Safeguarding requirements may be supplemented or modified between editions of Publication 1075 by guidance issued by the Office of Safeguards.

Live Data Testing Notification Requirements

Live Data Testing Notification Form

The use of live FTI in test environments should generally be avoided and is not approved unless specifically authorized by the IRS Office of Safeguards. Dummy data should be used in place of live FTI wherever possible. This memo provides guidance to federal, state and local agencies that receive, store, process or transmit FTI on the requirements for the approval, acquisition, handling, protection, and disposition of live FTI used in system testing activities. This guidance further expands upon the Live Data Testing requirements provided in IRS Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies, Section 9.4.6 – Live Data Testing.

Protecting FTI in a Cloud Computing Environment

Cloud Computing Notification Form

As agencies look to reduce costs and improve operations, cloud computing may offer promise as an alternative to traditional data center models. By utilizing software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) cloud service models, agencies may be able to reduce hardware and personnel costs by eliminating redundant operations and consolidating resources. While cloud computing offers many potential benefits, it is not without risk. Limiting access to authorized individuals becomes a much greater challenge with the increased availability of data in the cloud, and agencies may have greater difficulties isolating federal tax information (FTI) from other information and preventing “commingling” of data.

References/Related Topics

- Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities

- Safeguards Program