Internal Revenue Service Publication 1075 Compliance in AWS

First published February 2, 2018

Last updated February 24, 2021





Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. 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.

© 2022 Amazon Web Services, Inc. or its affiliates. All rights reserved.



Contents

Introduction	1
Our Commitment to Data Privacy	3
Security of the AWS Infrastructure	5
Mandatory Requirements for FTI in aCloud Environment	6
Creating an IRS 1075 Compliant Environment	12
Conclusion	15
Contributors	15
Document revisions	16



Abstract

AWS Customers receiving U.S. Federal Tax Information (FTI) are subject to requirements of the Internal Revenue Service (IRS) Publication 1075. The specific controls and architecture necessary to build solutions that are compliant with IRS 1075 are based largely on customer needs and configurations. This paper provides an overview of AWS service capabilities, including security services and tools that parties working with FTI can implement to help satisfy IRS 1075 requirements.



Introduction

The Internal Revenue Service Publication 1075 (IRS 1075) provides guidance to ensure that the policies, practices, controls, and safeguards employed by agencies, agents, or contractors who receive Federal TaxInformation (FTI) adequately protect the confidentiality and integrity of the FTI throughout its lifecycle.

IRS 1075 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. Besides written requests, 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.

The IRS Office of Safeguards is in place to promote taxpayer confidence in the integrity of the tax system by ensuring the confidentiality of IRS information provided to federal, state, and local agencies. Safeguards verifies compliance with IRC 6103(p)(4) safeguard requirements through the identification and mitigation of any risk of loss, breach, or misuse of Federal Tax Information held by external government agencies.

The Safeguards Program provides documented technical assistance which outlines the guidance that agencies should follow when securing FTI in a cloud environment. For more information, see the CloudComputing Environment page.

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.

As agencies look to reduce costs and improve operations, migrating workloads to AWS helps these customers streamline their processes and applications. The rest of this whitepaper provides you with the necessary background on AWS Security and Privacy controls and how you can implement controls necessary to build and manage IRS 1075 complaint workloads on AWS.



1

AWS provides you with services hosted in multiple U.S.-based Regions in which to build IRS 1075 workloads. These Regions include both our commercial AWS U.S. East and U.S. West Regions, which are authorized at the moderate baseline under the Federal Risk and Authorization Management Program (FedRAMP), and AWS GovCloud (US) East and West, which are authorized as the high baseline under FedRAMP. FedRAMP authorization includes assessment by an accredited independent third-party assessment organization (3PAO) and subsequent review and authorization by a federally authorized Joint Authorization Board (JAB). For an updated list of FedRAMP authorized services, see AWS Services in Scope by Compliance Program.



Our Commitment to Data Privacy

At AWS, earning customer trust is critically important to us. We deliver services to millions of active customers, including enterprises, educational institutions, and government agencies in over 190 countries. Our customers include financial services providers, healthcare providers, and governmental agencies, who trust us with some of their most sensitive information.

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

AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools our customers might need to meet their compliance needs, depending on their applications. We recommend that customers and APN Partners with general questions about AWS data protection services contact their AWS account manager first. If customers have signed up for Enterprise Support, they can reach out to their technical account manager (TAM) as well. TAMs work with solutions architects to help customers identify potential risks and potential mitigations. TAMs and account teams can also point customers and APN Partners with specific resources based on their environment and needs. AWS is not in the position to provide legal advice. We recommend that customers consult their legal counsel if they have legal questions.

Maintaining customer trust is an ongoing commitment. We strive to inform you of the privacy and data security policies, practices, and technologies we've put in place. These commitments include:

- Access As a customer, you maintain full control of your content and responsibility
 for configuring access to AWS services and resources. We provide an advanced set
 of access, encryption, and loggingfeatures to help you do this effectively (for
 example, AWS Identity and Access Management, AWS Organizations, and AWS
 CloudTrail). We provide API operations for you to configure access control
 permissions for any of the services you develop or deploy in an AWS environment.
- Storage You choose the AWS Regions in which your content is stored and the type
 of storage. You can replicate and back up your content in more than one AWS Region.



• **Encryption** – We offer you strong encryption for your content in transit and at rest. We also provide you with the option to manage your own encryption keys. These features include:

- Data encryption capabilities available in AWS storage and database services, such as Amazon ElasticBlock Store, Amazon Simple Storage Service (Amazon S3), Amazon Relational Database Service, (Amazon RDS) and Amazon Redshift.
- Flexible key management options, including AWS Key Management Service (KMS), allow you to choose whether to have AWS manage the encryption keys or enable you to keep complete controlover your keys.
- Server-side encryption (SSE) with Amazon S3-managed encryption keys (SSE-S3), SSE with AWS KMS-managed keys (SSE-KMS), or SSE with customer-provided encryption keys (SSE-C).
- Security services You can choose security services, which can automatically
 assess applications for exposure, vulnerabilities, and deviations from best practices
 and which you can configure to identify, analyze, and investigate potential security
 issues or findings, such as AWS Security Hub, Amazon GuardDuty, Amazon Macie,
 Amazon Inspector, and Amazon Detective.
- Disclosure of customer content We do not disclose your information unless we're
 required to do so in order to comply with a legally valid and binding order. Unless
 prohibited from doing so, or if there is clear indication of illegal conduct in connection
 with the use of AWS products or services, AWS notifies you before disclosing content
 information.
- Security assurance We have developed a security assurance program that uses best practices for global privacy and data protection to help you operate securely within AWS, and to make the best use of our security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments.

To learn more about AWS data privacy, see Data Privacy FAQ.



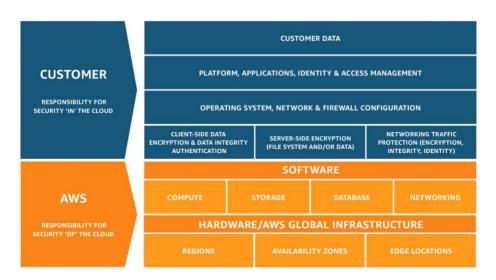
Security of the AWS Infrastructure

The AWS infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely.

This infrastructure is built and managed not only according to security best practices and standards, but also with the unique needs of the cloud in mind. AWS uses redundant and layered controls, nearly continuous validation and testing, and a substantial amount of automation to ensure that the underlying infrastructure is monitored and protected 24/7. AWS ensures that these controls are replicated in every new data center or service.

All AWS customers benefit from a data center and network architecture built to satisfy the requirements of our most security-sensitive customers. This means that you get a resilient infrastructure designed for high security, without the capital outlay and operational overhead of a traditional data center.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure and you are responsible for securing workloads, you deploy in AWS. This gives you the flexibility and agility you need to implement the most applicable security controls for your business functions in the AWS environment. You can tightly restrict access to environments that process sensitive data, or deploy less stringent controls for information you want to make public.



AWS Shared Responsibility Model

For more information, see Introduction to AWS Security and Shared Responsibility Model.



Mandatory Requirements for FTI in aCloud Environment

To utilize a cloud computing model to receive, transmit, store, or process FTI, the receiving party must be in compliance with all IRS 1075 requirements. Before introducing FTI to a cloud environment, the following mandatory requirements must be in effect:

1. **FedRAMP authorization** – Agencies maintaining FTI within cloud environments must utilize FedRAMP authorized services.

How AWS supports FedRAMP authorization:

AWS provides you with services hosted in multiple U.S.-based Regions in which to build IRS 1075 workloads. These Regions include both our commercial AWS U.S. East and U.S. West Regions, which are authorized at the moderate baseline under the Federal Risk and Authorization Management Program (FedRAMP), and AWS GovCloud (US) East and West, which are authorized at the high baseline under FedRAMP. FedRAMP authorization includes assessment by an accredited independent third- party assessment organization (3PAO) and subsequent review and authorization by a federally authorized Joint Authorization Board (JAB). For an updated list of FedRAMP authorized services, see AWS Services in Scope by Compliance Program.

2. **Onshore access** – Agencies must use vendors and services where all FTI physically resides in systems located within the United States, and all access and support of such data is performed from the United States.

How AWS supports onshore access:

All AWS (US) Regions are physically located in the continental United States. For more information, see the AWS Global Infrastructure Map. The use of AWS services does not require authorized access to FTI. As such, no authorized disclosure is required, as outlined in IRS 1075, Section 11.2. You retain complete control of your data and can set and control all access to your virtual environment to permit only the use of services in U.S. Regions and connections from the U.S.

3. **Physical description** – Agencies and their cloud providers must provide a complete listing of all data centers within the cloud environment where FTI will be received, processed, transmitted, or stored.

How AWS supports physical description:



AWS has provided the IRS with applicable data center location information under NDA. So, you need only to provide data center Regions you are using. General data center location information is listed (by country, region/state, city) in the PCI-DSS compliance report which can be downloaded by AWS customers from the AWS Management Console using AWS Artifact.

4. **Notification requirement** – The agency must notify the IRS Office of Safeguards at least 45 days prior to transmitting FTI into a cloud environment.

How AWS supports notification requirements:

AWS Sample IRS Cloud Computing Notification Form – Upon request, AWS can provide sample language to help guide agencies in completing the Cloud Computing Notification Form.

5. **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:

- Customers using AWS can benefit from a data center, network, and software
 architecture built to satisfy the requirements of the most security-sensitive
 organizations in the world. AWS provides highly available services and
 supports a combination of traditional and novel security mechanisms that are
 intrinsic to its service design and operation.
- AWS gives you rich control over your content and provides tools to determine where your content will be stored and how it will be protected. AWS features provide you the ability to secure your content in transit and at rest, to tightly control access to AWS services and resources for your users, and to monitor access as well as the evolving state of your systems. You maintain full control over access to your content, and have the ability to build access control mechanisms to prevent unauthorized users from accessing your data. All this occurs within a framework of multi-tenant services with strict logical isolation. The logical isolation between customer environments provided by AWS can be more effective and reliable than security seen in dedicated physical infrastructure. For more information, see Logical Separation on AWS.



 Service level agreements (SLA) – The agency must establish security policies and procedures based on IRS 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 protects against improper actions in support of IRS 1075 workloads:

In addition to the controls outlined in this paper, details about data privacy, data ownership, control of customer content, roles, and responsibilities and service availability are detailed in AWS Service Terms, AWS Service Level Agreements and AWS Customer Agreement.

7. **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 the FIPS 140-2 compliant modules. This requirement must be included in the cloud vendor's agreement.

How AWS supports data encryption in transit for IRS 1075 workloads:

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. 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 encryption. AWS works with customers to provide the information they need to help manage compliance when building on AWS services.

AWS Key Management Service (AWS KMS) is FIPS 140-2 compliant. AWS KMS NIST certificates are:#3617, #3139, and #3009.

8. 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 the FIPS 140-2 compliant module. This requirement must be included in the SLA, if applicable.

How AWS supports data encryption at rest for IRS 1075 workloads:



AWS KMS is seamlessly integrated with several other AWS services. This
integration means that you can use AWS KMS master encryption keys to
encrypt the data you store when using 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 created in
AWS KMS and have permission to use. AWS KMS has also been FIPS 140-2
validated, a requirement for many federal, state, and local organizations to use
cryptographic modules and hardware security modules (HSMs).

- As your usage of AWS KMS encryption keys grows, you don't have to buy additional key management infrastructure. AWS KMS automatically scales to meet your encryption key needs. The master keys created on your behalf by AWS KMS or imported by you can't be exported from the service. AWS KMS stores multiple copies of encrypted versions of your keys in systems that are designed for 99.99999999% durability to help assure you that your keys will be available when you need to access them. If you import keys into AWS KMS, you must securely maintain a copy of your keys so that you can re-import them at any time. AWS KMS is deployed in multiple Availability Zones within an AWS Region to provide high availability for your encryption keys.
- 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 AWS.
- To learn more about how AWS KMS works, see AWS Key Management Service Cryptographic Details.
- Amazon EC2 instances built on the AWS Nitro System also offer FIPS 140-2 validated encryption under NIST Certificate #3739.
- 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). This requirement must be included in the cloud vendor's agreement.

How AWS supports data sanitizing requirements for IRS 1075 workloads:



AWS uses the techniques detailed in DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. Additionally, you are responsible for data sanitization of your data volumes and can run the same techniques outlined in DoD 5220.22-M and NIST 800-88.

10. 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.

How AWS supports risk assessment requirements for IRS 1075 workloads:

You should include your use of AWS services within their annual risk assessment processes. For more information, see Amazon Web Services: Risk and Compliance.

11. **Multi-factor authentication** – Cloud implementations that truly represent remote access from the internet must incorporate multi-factor authentication.

How AWS supports multi-factor authentication:

- AWS Multi-Factor Authentication (MFA) is a simple best practice that adds an extra layer of protection on top of your user name and password. With MFA enabled, when a user signs in to an AWS Management Console, they will be prompted for their user name and password (the first factor
- —what they know), as well as for an authentication code from their AWS MFA device (the second factor—what they have). Taken together, these multiple factors provide increased security for your AWS account settings and resources.
- Identity federation in AWS enables you to manage access to your AWS
 resources centrally. With federation, you can use single sign-on (SSO) to
 access your AWS accounts using credentials from your corporate directory.
 Federation uses open standards, such as Security Assertion Markup Language
 2.0 (SAML), to exchange identity and security information between an identity
 provider(IdP) and an application.



 AWS offers multiple options for federating your identities in AWS. You can use AWS Identity and Access Management (IAM) to enable users to sign in to their AWS accounts with their existing corporate credentials. You also can add federation support to your own web and mobile applications by using Amazon Cognito.

- AWS also offers non-SAML-based options for managing access to your AWS resources. AWS Directory Service for Microsoft Active Directory, also known as AWS Microsoft Managed AD, uses secure Windows trusts to enable users to sign in to the AWS Management Console, AWS CommandLine Interface (AWS CLI), and Windows applications running on AWS using Microsoft Active Directory credentials.
- 12. **Security control implementation** Customer-defined security controls must be identified, documented, and implemented. The customer defined security controls, as implemented, must comply with IRS 1075 requirements.

How AWS supports security control implementation requirements for IRS 1075 workloads:

- You can leverage AWS's FedRAMP packages and authorizations in order to accelerate your Security Assessment and Authorization (SA&A) efforts. AWS provides you with a package of security guidance and documentation to enhance your understanding of security and compliance while using AWS services.
- For example, AWS provides an SSP template based upon NIST 800-53, 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.
- U.S. Government customers can request access to the AWS FedRAMP
 Security Package from the FedRAMP PMO by completing a Package Access
 Request Form and submitting it to <info@fedramp.gov>, or contacting their
 AWS Sales Account Manager.
- APN Partners and prospective customers can also request access to the AWS FedRAMP Security Package by contacting their AWS Sales Account Manager.



Creating an IRS 1075 Compliant Environment

AWS provides several resources that can help you meet the requirements of various compliance frameworks, including IRS 1075, when using AWS services. You can leverage AWS security features and functions, and leading industry best practices, to help you architect and IRS 1075-compliant solution with FTI in the cloud. This section provides a high-level overview of services and tools agencies, agents, or contractors should consider as part of their IRS 1075 implementation on AWS.

- Built-in firewalls You can control how accessible your instances are by configuring built-in firewall rules, from totally public to completely private, or somewhere in between.
- 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 your corporate directory service, such as Active Directory.
- Guest operating system You control access to virtual instances in Amazon EC2 and Amazon Virtual Private Cloud (Amazon VPC). You have full administrative access and control over these accounts, services, and applications.
 - Although AWS provides images that can be used for deployment of host operating systems, you need to develop and implement system configuration and hardening standards to align with all applicable IRS 1075 requirements for your operating systems.
- Storage AWS provides various options for storage of information including Amazon Elastic BlockStore (EBS), Amazon S3, and Amazon Relational Database Service (Amazon RDS). These services enable you to make data easily accessible to your applications and for backup purposes. To meet IRS 1075 requirements for restricting direct inbound and outbound access to systems that contain sensitive data, the storage of sensitive data in the various storage options should consider the technology and accessibility of the data to the internet.

For example, you can configure Amazon S3 to require the use of 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.



 Private subnets – Amazon VPC allows you to add another layer of network security to your instances by creating private subnets and adding an IPSec VPN tunnel between your home network and your Amazon VPC.

- Encrypted data storage You can have the data and objects you store in Amazon EBS, Amazon S3, Amazon S3 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.
- Dedicated connection option The AWS Direct Connect service allows you to
 establish a dedicated network connection from your premises to AWS. Using industry
 standard 802.1q VLANs, this dedicated connection can be partitioned into multiple
 logical connections to enable you to access both public and private IP environments
 within the AWS Cloud.
- Security logs AWS CloudTrail makes it easier to ensure compliance with internal policies and regulatory standards by providing a history of activity in your AWS account. AWS CloudTrail provides event history of your AWS account activity, including actions taken through the AWS Management Console, AWS SDKs, command line tools, and other AWS services.
- Asset identification and configuration With the AWS Config service, you can immediately discoverall your AWS resources and view the configuration of each. You can receive notifications each time aconfiguration changes, as well as dig into the configuration history to perform incident analysis.
- Centralized key management If you use encryption extensively and require strict control of your keys, the AWS Key Management Service (AWS KMS) provides a convenient management option for creating and administering the keys used to encrypt your data at rest.
- **AWS CloudHSM** If you must use Hardware Security Module (HSM) appliances for cryptographic keystorage, AWS CloudHSM provides a highly secure and convenient way to store and manage keys.
- AWS Trusted Advisor Provided automatically when you sign up for premium support, AWS Trusted Advisor is a convenient way for you to see where you could use a little more security. It monitors AWS resources and alerts you to security configuration gaps, such as overly permissive access to certain Amazon EC2 instance ports and Amazon S3 storage buckets, minimal use of role segregation using IAM, and weak password policies.



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



Conclusion

This whitepaper has summarized AWS service capabilities, including security services and tools, which parties working with FTI can implement to help them meet IRS 1075 requirements.

AWS Compliance enables understanding of the robust controls in place at AWS to maintain security and data protection in the cloud. As systems are built on top of AWS Cloud infrastructure, compliance responsibilities will be shared. By tying together IRS 1075 governance-focused, audit-friendly service features with applicable security compliance regulations or audit standards, AWS Compliance enables you to build on traditional programs and assists you in establishing and operating in an AWS security control environment.

Contributors

Contributors to this document include:

- Stephen Exley, Industry Specialist, AWS Security
- Patrick Woods, Senior Security Specialist, AWS Security
- Ted Steffen, Senior Security Partner Strategist, AWS Public Sector
- Greg Herrmann, Senior Security Partner Strategist, AWS Public Sector
- Eric Schwenter, Senior Manager Solutions Architecture, AWS Public Sector



Document revisions

Date	Description
February 24, 2021	Updated for technical accuracy.
February 2, 2018	First publication

