Internal Revenue Service Publication 1075 Compliance in AWS

August 2024

aws

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 Amazon Web Services (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.

Contents

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 Tax Information (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 Cloud Computing 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 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 compliant workloads on AWS.

AWS provides customers 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 the FedRAMP Board. For an updated list of FedRAMP authorized services, see the AWS Services in Scope by Compliance Program page.

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 more than 200+ countries. Our customers include financial services providers, healthcare providers, and governmental agencies, who trust us with some of their most sensitive information.

AWS knows that customers care deeply about privacy and data security. That's why AWS gives customers ownership and control over their content through simple, powerful tools that allow you to determine where their content will be stored, secure their content in transit and at rest, and manage their access to AWS services and resources for customer's users.

AWS also implements sophisticated technical and physical controls designed to prevent unauthorized access to or disclosure of customer's content.

AWS continually monitors the evolving privacy regulatory and legislative landscape to identify changes and determine what tools customers might need to meet their compliance needs, depending on their applications.

AWS recommends that customers and AWS Partner Network (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 mitigations associated with a variety of solutions and deployments. TAMs and account teams can also provide 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. Guidance and applicability to IRS 1075 requirements are discussed in the Mandatory Requirements for FTI in a Cloud Environment section below. Generally, AWS has built important privacy and data security policies, practices, and technologies that include:

- **Access** – Customers maintain control of their content and responsibility for configuring access to AWS services and resources. AWS provides an advanced set of access, encryption, and logging features to help customers do this effectively (for example, AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS), and AWS CloudTrail). AWS provides Application Program Interface (API) operations for customers to use to configure access control permissions for any of the services customers develop or deploy in an AWS environment.

- **Locality** – Customers may specify the AWS Regions from across the globe in which their workloads (content and services) will be stored and operated. Customers can replicate and back up their content in more than one AWS Region or AWS Availability Zone. Additionally, customers can use AWS Organizations for improved account management and consolidated billing capabilities that enables customers to better meet budgetary, security, and compliance needs of their business.

- **Security** – Customers choose how their content is secured. AWS helps organizations to develop and evolve security, identity, and compliance into key business enablers. At AWS, security is our top priority. AWS is architected to be the most secure global cloud infrastructure on which to build, migrate, and manage applications and workloads. Customers manage their implementation of AWS security services. For example, AWS Security Hub, Amazon GuardDuty, Amazon Macie, Amazon Inspector, and Amazon Detective which can automatically assess applications for exposure, vulnerabilities, and deviations from best practices. These security services support customers in the identification, analysis, and investigation of potential security issues or findings.

- **Disclosure of customer content** – AWS does not disclose a customer's information unless required to comply with law or binding government order.

- **Security Assurance** – AWS has developed a security assurance program that uses best practices for global privacy and data protection to help customers operate securely within AWS, and to make the best use of AWS's security control environment. These security protections and control processes are independently validated by multiple third-party independent assessments. For additional IRS1075 guidance, visit the AWS compliance IRS1075 web page.

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

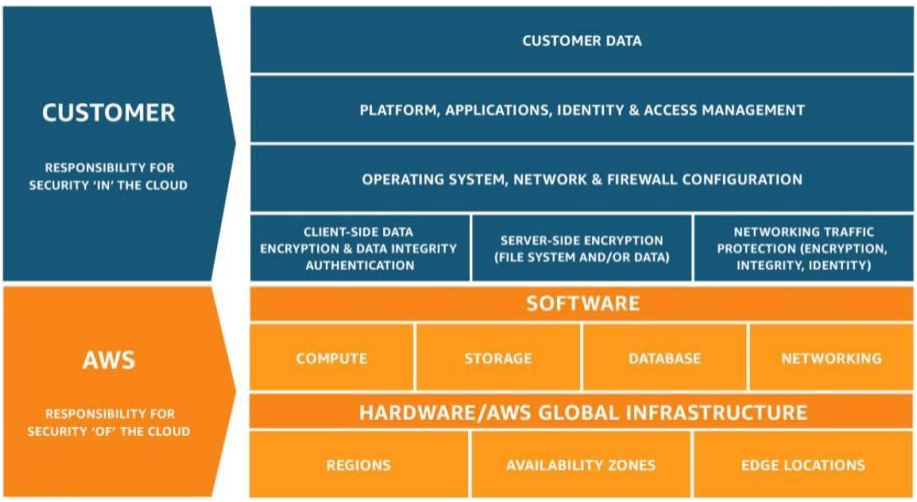
cloud computing environments available today. It is designed to provide an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely, and to customize controls to satisfy security requirements, such as those in IRS 1075.

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 throughout the AWS infrastructure.

AWS operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (of the cloud) and customers are responsible for securing the workloads they deploy in AWS (in the cloud). The AWS Shared Responsibility Model is fundamental to understanding the respective roles of the customer and AWS in the context of cloud security principles and how a customer can architect a solution in compliance with applicable regulatory requirements, such as IRS 1075.

This model gives customers the flexibility and agility they need to implement the most applicable security controls for their business functions in the AWS environment.

Customers can tightly restrict access to environments that process sensitive data or deploy less stringent controls for information they 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 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 1075 requirements. Before introducing FTI into 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 customers with services hosted in multiple U.S.-based Regions in which to build IRS 1075 workloads. These Regions include both commercial AWS U.S. East and U.S. West Regions, which are authorized at the FedRAMP moderate baseline, and AWS GovCloud (US) East and West, which are authorized at the FedRAMP high baseline. FedRAMP authorization includes assessments by a 3PAO and subsequent review and authorization by the FedRAMP Board. 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:

   AWS' US Regions are physically located in the continental United States. For more information, see the AWS Services by Region page and filter for the US regions.

   The use of AWS services does not require AWS to have authorized access to FTI. As such, no authorized disclosure is required, as outlined in IRS 1075, Section 11.2. Customers retain complete control of their data and can set and control all access to their 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. Customers need only to provide data center Regions they 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 provides customers rich control over their content and provides tools to determine where their content will be stored and how it will be protected. AWS features provide customers the ability to secure their content in transit and at rest, to tightly control access to AWS services and resources for their users, and to monitor access as well as the evolving state of their systems. Customers maintain full control over access to their content and have the ability to build access control mechanisms to prevent unauthorized users from accessing their 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 a dedicated physical infrastructure. For more information, see Logical Separation on AWS.

6. **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 use the latest FIPS-140 validated mechanism and operate utilizing the FIPS-140 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 and FIPS 140-3 are U.S. government security standards that specify security requirements for cryptographic modules protecting sensitive information. To support customers with FIPS 140 requirements, the Amazon Virtual Private Cloud VPN endpoints and SSL terminations in AWS GovCloud (US) operate using FIPS 140 validated encryption. AWS works with customers to provide the information they need to help manage compliance when building on AWS services.

   For more information on FIPS validated endpoints or the latest FIPS certificates, visit the FIPS Compliance page or contact your AWS account manager.

   Note that AWS is mandating TLS 1.2 connections for customers dependent on FedRAMP or who must meet U.S. Government requirements. For additional guidance on TLS and AWS endpoints, view this AWS Security Blog.

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 use the latest FIPS-140 validated encryption mechanism. This requirement must be included in the SLA, if applicable.

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

   - AWS KMS and customer managed keys (CMK) are seamlessly integrated with several other AWS services. This integration means that customers can use

AWS KMS master encryption keys to encrypt the data they store when using AWS services. Customers can use a default master key that is created for customers automatically and usable only within the integrated service, or customers can select a custom master key that the customer created in AWS KMS and have permission to use. Customer managed keys are KMS keys in the AWS account that customers create, own, and manage. Customers have full control over their KMS/CMK keys. AWS KMS has also been FIPS 140 validated, a requirement for many federal, state, and local organizations to use cryptographic modules and hardware security modules (HSMs).

- As customer usage of AWS KMS encryption keys grows, customers don't have to buy additional key management infrastructure. AWS KMS automatically scales to meet customer encryption key needs. The master keys created on the customers behalf by AWS KMS or imported by the customer cannot be exported from the service. AWS KMS stores multiple copies of encrypted versions of a customer's keys in systems that are designed for 99.999999999% durability to help assure customers that their keys will be available when they need to access them. If customers import keys into AWS KMS, the customer must securely maintain a copy of their keys so that they can re-import them at any time. AWS KMS is deployed in multiple Availability Zones within an AWS Region to provide high availability for customer 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 customer's 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.

9. **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, customers are responsible for data sanitization of their 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:

    Customers should include their 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 a customer's username and password. With MFA enabled, when a customer user signs in to an AWS Management Console, they will be prompted for their username 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 a customer's AWS account settings and resources.

    - Identity federation in AWS enables customers to manage access to their AWS resources centrally. With federation, customers can use single sign-on (SSO) to access their AWS accounts using credentials from their 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 customer identities in AWS. Customers can use AWS Identity and Access Management (IAM) to enable users to sign in to their AWS accounts with their existing corporate credentials. Customers can also add federation support to their own web and mobile applications by using Amazon Cognito.

    - AWS also offers non-SAML-based options for managing access to customer 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 Command Line 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:

    - Customers can leverage AWS's FedRAMP packages and authorizations 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 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.
    - AWS Artifact provides on-demand access to AWS' security and compliance reports, enabling customers to assess the compliance status of their AWS environment and demonstrate adherence to regulations. Customers can use AWS Artifact (the automated compliance reporting portal available in the AWS Management Console) to review and download reports and details about more than 2,500 security controls. The AWS Artifact portal provides on-demand access to AWS security and compliance documents, as well as certifications and attestations from accreditation bodies across geographies and compliance verticals, including Service Organization Control (SOC) reports, International Organization for Standardization (ISO) reports, Payment Card Industry (PCI) reports, Federal Risk and Authorization Management Program (FedRAMP), FedRAMP Authorization, and Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR), to name a few.

Creating an IRS 1075 Compliant Environment

AWS provides resources that can help customers meet the requirements of various compliance frameworks, including IRS 1075, when using AWS services. Customers can leverage AWS security features and functions, and leading industry best practices, to help them to architect an 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. This is not a complete and comprehensive list of all services that can be used to align a customer's workloads to IRS 1075.

- **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.
- **Authentication and authorization** – There are two layers of authentication and authorization to consider in a customer's AWS environment: IAM credentials and AWS customer-controlled credentials. IAM provides authentication and authorization for direct access to AWS services by using either local IAM accounts or integrating access controls with a customer's corporate directory service, such as Active Directory.
- **Guest operating system** – Customer's control access to virtual instances in Amazon EC2 and Amazon Virtual Private Cloud (Amazon VPC). Customers have full administrative access and control over these accounts, services, and applications.

  The AWS Nitro System is the foundation for our next generation of EC2 instances that enables AWS to innovate faster, further reduce cost for our customers, and deliver added benefits like increased security and new instance types. The Nitro System provides enhanced security that continuously monitors, protects, and verifies the instance hardware and firmware. Virtualization resources are offloaded to dedicated hardware and software minimizing the attack surface. Nitro System's security model is locked down and prohibits administrative access, eliminating the possibility of human error and tampering.

  Although AWS provides images that can be used for deployment of host operating systems, customers must develop and implement system configuration and hardening standards to align with all applicable IRS 1075 requirements for their operating systems.
- **Storage** – AWS provides various options for storage of information including Amazon Elastic Block Store (EBS), Amazon S3, and Amazon Relational Database Service (Amazon RDS). These services enable customers to make data easily accessible to their 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, customers 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 customers to add another layer of network security to their instances by creating private subnets and adding an IPSec VPN tunnel between a customer's home network and their Amazon VPC.
- **Encrypted data storage** – Customers can have the data and objects they 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 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.
- **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 a customer's 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, customers can immediately discover all 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.
- **Centralized key management** – If customers 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 their data at rest.
- **AWS CloudHSM** – If customers 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 Trusted Advisor** – Provided automatically when customers sign up for premium support, AWS Trusted Advisor is a convenient way for customers to see where they could use a little more security. It monitors AWS resources and alerts customers 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 customers select the best options for their 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 customers to build on traditional programs and assists in establishing and operating IRS 1075 compliant workloads in an AWS security control environment.

Contributors

Contributors to this document include:

- Robert Siple, Security Assurance Specialist, AWS Security
- Stephen Exley, Security Industry Specialist, AWS Security
- Ted Steffan, Senior Security Partner Strategist, AWS Public Sector
- Eric Schwenter, Senior Manager Solutions Architecture, AWS Public Sector
- Kevin Murakoshi, Principal Solution Architect, AWS WWPS EDU/SLG
- Abhijeet Lokhande, Sr. Solution Architect, AWS WWPS EDU/SLG

Services Links

The following provides links to the referenced Amazon and AWS services noted within this document:

- Amazon Cognito
- Amazon Detective
- Amazon EC2
- Amazon Elastic Block Store (EBS)
- Amazon GuardDuty
- Amazon Inspector
- Amazon Macie
- Amazon Redshift
- Amazon Relational Database Service (Amazon RDS)
- Amazon S3
- Amazon S3 Glacier
- Amazon Virtual Private Cloud (Amazon VPC)
- AWS Artifact
- AWS CloudHSM
- AWS CloudTrail
- AWS Command Line Interface (AWS CLI)
- AWS Config
- AWS Direct Connect
- AWS Identity and Access Management (IAM)
- AWS KMS
- AWS Microsoft Managed AD
- AWS Multi-Factor Authentication (MFA)
- AWS Organizations
- AWS Partner Network (APN)
- AWS Security Hub
- AWS Trusted Advisor
- AWS Trusted Advisor

Additional Resources

AWS Partner Network (APN)

The AWS Partner Network (APN) is the global partner program for AWS. The program focuses on helping APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support.

APN includes AWS Security Competency Partners, which are APN Partners that have demonstrated deep technical expertise with security in AWS and proven customer success securing the cloud journey with their software and services offerings. By working with these AWS Security Competency Partners, customers receive greater access to innovative, cloud-based solutions.

For more information, refer to AWS Security Competency Partners.

AWS Managed Services (AMS)

AWS Managed Services (AMS) helps customers adopt AWS at scale and operate more efficiently and securely. We leverage standard AWS services and offer guidance and execution of operational best practices with specialized automations, skills, and experience that are contextual to your environment and applications. AMS provides proactive, preventative, and detective capabilities that raise the operational bar and help reduce risk without constraining agility, allowing you to focus on innovation. AMS extends your team with operational capabilities including monitoring, incident management, AWS Incident Detection and Response, security, patch, backup, and cost optimization. AWS Incident Detection and Response is available in English for workloads hosted in eligible AWS regions.

For more information, refer to AWS Managed Services.

AWS Professional Services (ProServe)

Adopting the AWS Cloud can provide organizations with sustainable business advantages. Supplementing your team with specialized skills and experience can help you achieve those results. The AWS Professional Services is a global team of experts that can help customers realize their desired business outcomes when using the AWS Cloud. ProServe works with your team and your chosen member of the AWS Partner Network (APN) to execute and realize your enterprise cloud computing initiatives.

For more information, refer to AWS Professional Services.

Further Reading

For additional information, refer to:

- AWS Documentation
- AWS Security Documentation
- AWS Compliance
- Amazon Web Services: Overview of Security Processes
- IRS Safeguards Program

Document Revisions

Date	Description
August 2024	Review and refresh for technical accuracy.
February 24, 2021	Updated for technical accuracy.
February 2, 2018	First publication