AWS SECURITY AND COMPLIANCE

QUICK REFERENCE GUIDE

This document has been archived.

For the latest technical content, see:
https://aws.amazon.com/compliance

Education Edition

2018

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.

We think differently about security and compliance.

As with everything at Amazon, the success of our security and compliance program is primarily measured by one thing: our customers' success. Our customers drive our portfolio of compliance reports, attestations, and certifications that support their efforts in running a secure and compliant cloud environment.

You can take advantage of this effort to achieve the savings and scalability that AWS offers while still maintaining robust security and regulatory compliance.

Overview

Overview

Security at AWS is our top priority. Nothing is more important to us than protecting your data. As an AWS customer, you will benefit from a data center and network architecture built to meet the requirements of the most security-sensitive organizations.

> *"Our biggest concern was making sure we keep our students' data secure – and we've done that with our move to the AWS Cloud."*
>
> **- William Dembi**
> Infrastructure Specialist, IDL

We innovate rapidly at scale, continually incorporating your feedback into AWS services. This benefits you because our solutions improve over time, including constantly evolving core security services such as identity and access management, logging and monitoring, encryption and key management, network segmentation, and standard DDoS protection at little to no additional cost.

You also get advanced security services invented by engineers with deep insight into global security trends, allowing your team to proactively address emerging risks in real time while paying for only what you use all at a lower cost. This means you can choose the security that meets your needs as you grow, without upfront expenses and with much lower operational overhead when compared to managing your own infrastructure.

Overview

A properly secured environment results in a compliant environment. When you migrate your regulated workloads to the AWS cloud, you can achieve a higher level of security at scale by using our many governance-enabling features. Cloud-based governance offers lower cost of entry, easier operations, and improved agility by providing more oversight, security control, and central automation.

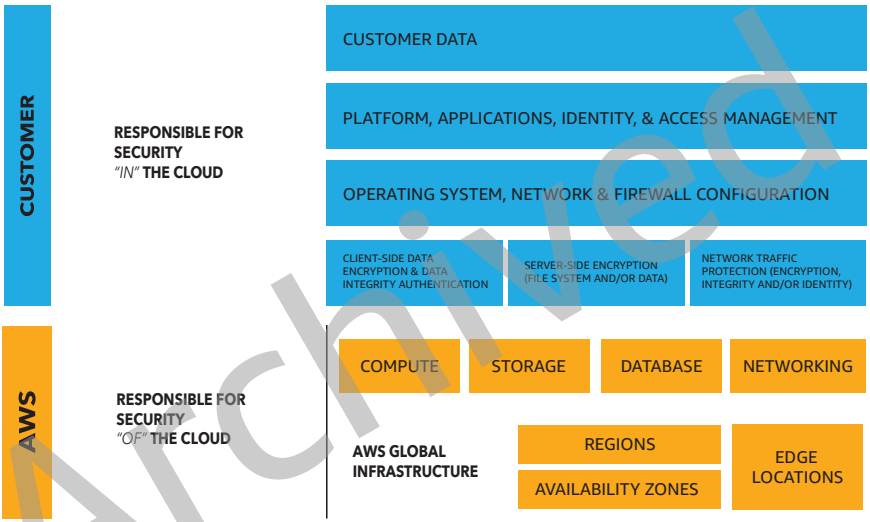
> *"We were able to get the cloud infrastructure up and running in a record amount of time, at a much lower cost than we could have done ourselves."*
>
> **- Mark Field**
> CTO, Thermo Fisher Scientific

By using AWS, you inherit the many security controls that we operate, thus reducing the number of security controls that you need to maintain. Your own compliance and certification programs are strengthened while at the same time lowering your cost to maintain and run your specific security assurance requirements.

How We Share Responsibility

HOW WE SHARE RESPONSIBILITY

When you move your IT infrastructure to AWS, you will adopt the model of shared responsibility shown below. Because we operate, manage, and control the IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate, this shared model reduces your operational burden.



Shared Responsibility Model

Just as you share the responsibility for operating the IT environment with us, you also share the management, operation, and verification of IT controls. We reduce your burden on operating controls by managing those controls associated with the physical infrastructure deployed in the AWS environment.

AWS - Security of the Cloud

In order to help you establish, operate and leverage our security control environment, we have developed a security assurance program that uses global privacy and data protection best practices. These security protections and control processes are independently validated by multiple third-party independent assessments. Our assurance program is based on **Validating**, **Demonstrating**, and **Monitoring**.

We **Validate** that our services and facilities across the globe maintain a ubiquitous control environment that is operating effectively. Our control environment includes policies, processes and control activities that leverage various aspects of Amazon's overall control environment.

The collective control environment encompasses the people, processes, and technology necessary to establish and maintain an environment that supports the operating effectiveness of our control framework. We have integrated applicable cloud-specific controls identified by leading cloud computing industry bodies into our control framework. We monitor these industry groups to identify leading practices that you can implement, and to better assist you with managing their control environment.

AWS - Security of the Cloud

We **Demonstrate** our compliance posture to help you verify compliance with industry and government requirements. We engage with external certifying bodies and independent auditors to provide you with considerable information regarding the policies, processes, and controls established and operated by us. You can leverage this information to perform your control evaluation and verification procedures, as required under the applicable compliance standard.

We **Monitor** that, through the use of thousands of security control requirements, we maintain compliance with global standards and best practices.

You can use services such as AWS Config to monitor the security and compliance of your environment.

AWS Config

AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance.

With AWS Config, you can discover existing and deleted AWS resources, determine your overall compliance against rules, and dive into configuration details of a resource at any point in time. These capabilities enable compliance auditing, security analysis, resource change tracking, and troubleshooting.

Customer - Security in the Cloud

Much like a traditional data center, you are responsible for managing the guest operating system (including installing updates and security patches) and other associated application software, as well as the configuration of the AWS-provided security group firewall. Your responsibilities will vary depending on the services you use, the integration of those services into your IT environment, and applicable laws and regulations. You should take all of this in consideration as you choose the AWS services that you will use.

In order to securely manage your AWS resources, you need to know what resources you are using (asset inventory), securely configuring the guest OS and applications on your resources (secure configuration settings, patching, and anti-malware), and control changes to the resources (change management).

You can incorporate the information that we provide about our risk and compliance program into your governance framework.

AWS Service Catalog

You can use AWS Service Catalog to create and manage catalogs of IT services that you have approved for use on AWS, including virtual machine images, servers, software, and databases to complete multi-tier application architectures. AWS Service Catalog allows you to centrally manage commonly deployed IT services, and helps you achieve consistent governance and meet your compliance requirements, while enabling users to quickly deploy only the approved IT services they need.

Assurance Programs

Assurance Programs

We categorize programs by Certifications/Attestations, Laws, Regulations, and Privacy, and Alignments/Frameworks.

Certifications/Attestations such as PCI DSS and ISO 27001 are performed by a third-party independent auditor. Our certifications, audit reports, or attestations of compliance are based on the results of the auditor's work.

Laws/Regulations/Privacy and Alignments/Frameworks such as HIPAA and FERPA are specific to your industry or function. We support you by providing functionality such as security features and enablers such as compliance playbooks, mapping documents, and whitepapers. Formal "direct" certification of these laws, regulations and programs is either:

- Not available to cloud providers or
- Represents a smaller subset of requirements already demonstrable by our current formal certification/ attestation programs.

Our environments are continuously audited, and our infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and verticals. You can use these certifications to validate the implementation and effectiveness of our security controls. We are continually adding programs. For the most current list visit the AWS Assurance Programs website.

Assurance Programs

PCI DSS – AWS, being a PCI DSS "Compliant" Service Provider (since 2010), means that if you use AWS products and services to store, process or transmit cardholder data, you can rely on our technology infrastructure as you manage your own PCI DSS compliance certification.

ISO 27001 – ISO 27001 is a widely adopted global security standard that outlines the requirements for information security management systems. It provides a systematic approach to managing company and customer information that's based on periodic risk assessments.

AWS Artifact

You can review and download reports and details about more than 2,500 security controls by using AWS Artifact, our automated compliance reporting tool available in the AWS Management Console.

AWS Artifact provides on-demand access to our security and compliance documents, also known as audit artifacts. You can use the artifacts to demonstrate the security and compliance of your AWS infrastructure and services to your auditors or regulators.

Examples of audit artifacts include ISO 27001:2013 and Payment Card Industry (PCI) reports.

Assurance Programs

FedRAMP – A U.S. government program for ensuring standards in security assessment, authorization, and continuous monitoring. FedRAMP follows NIST and FISMA defined control standards.

AWS offers FedRAMP compliant systems that have been granted authorizations, address the FedRAMP security controls, use required FedRAMP templates for the security packages posted in the secure FedRAMP Repository, have been assessed by an accredited independent third-party assessor (3PAO) and maintain continuous monitoring requirements of FedRAMP.

HIPAA – The Health Insurance Portability and Accountability Act (HIPAA) contains strict security and compliance standards for organizations processing or storing Protected Health Information (PHI). AWS enables covered entities and their business associates subject to HIPAA to leverage the secure their AWS environment to process, maintain, and store PHI.

FERPA – The primary intent of Family Educational Rights and Privacy Act (FERPA) is to protect student identities and the privacy of student records related to educational records, PII, and directory information. AWS enables covered institutions to comply with FERPA by providing capabilities to securely store and protect student data.

Securing Your Content

Securing Your Content

AWS is vigilant about your privacy. You always own your content, including the ability to encrypt it, move it, and manage retention. We provide tools that allow you to easily encrypt your data in transit and at rest to help ensure that only authorized users can access it.

Key Management Service

AWS Key Management Service (KMS) is a managed service that makes it easy for you to create and control the encryption keys used to encrypt your data, and uses Hardware Security Modules (HSMs) to protect the security of your keys. AWS Key Management Service is integrated with AWS CloudTrail to provide you with logs of all key usage to help meet your regulatory and compliance needs.

Server-Side Encryption

You can use Amazon S3 Server Side Encryption (SSE) if you prefer to have Amazon S3 manage the encryption process for you. Data is encrypted with a key generated by AWS or with a key you supply, depending on your requirements. With Amazon S3 SSE, you can encrypt data on upload simply by adding an additional request header when writing the object. Decryption happens automatically when data is retrieved.

Securing Your Content

These tools also give you the control you need to comply with regional and local data privacy laws and regulations. The design of our global infrastructure allows you to retain complete control over the regions in which your data is physically located, helping you meet data residency requirements.

> **Note**: We do not access or use your content for any purpose other than to provide you and your end users with the selected AWS services. We never use your content for our own purposes, including marketing or advertising.

With AWS, you know who is accessing your content, and what resources your organization is consuming at any given moment. Fine-grain identity and access controls combined with continuous monitoring for near real-time security information ensure that the right resources have the right access at all times, regardless of where in the world your information is stored.

AWS Identity Access Management

AWS Identity and Access Management (IAM) is central to securely controlling access to AWS resources. Administrators can create users, groups, and roles with specific access policies to control which actions users and applications can perform through the AWS Management Console or AWS API. Federation allows IAM roles to be mapped to permissions from central directory services.

Federated User Access

Federated users are users (or applications) who do not have AWS Accounts. With roles, you can give them access to your AWS resources for a limited amount of time. This is useful if you have non-AWS users that you can authenticate with an external service, such as Microsoft Active Directory, LDAP, or Kerberos.

AWS CloudTrail

AWS CloudTrail records AWS API calls and delivers log files that include caller identity, time, source IP address, request parameters, and response elements. You can use the call history and details that CloudTrail provides to enable security analysis, resource change tracking, and compliance auditing.

Reduce risk and enable growth by using our activity monitoring services that detect configuration changes and security events across your ecosystem, even integrating our services with your existing solutions to simplify your operations and compliance reporting.

Securing Your Content

Amazon GuardDuty

Amazon GuardDuty provides threat intelligence and monitoring of a customer's account and VPC resources. The service can be used to detect mis-configurations in a customer's account, provide threat intelligence such as instances communicating with known bad actors as well as alerting and automating to remediate these issues.

Amazon Macie

Amazon Macie provides data classification and data access information to help ensure data is appropriately handled and accessed. This service allows customers to have better insight into what data they are storing and how it's being accessed and exposed.

Amazon Inspector

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

We do not disclose your content, unless we're required to do so to comply with the law or a valid and binding order of a governmental or regulatory body. In the case where we are required to disclose your content, we first notify you so that you can seek protection from discloser.

> **Important**: If we are prohibited from notifying you, or there is clear indication of illegal conduct in connection with the use of Amazon products or services, we will not notify you before disclosing your content.

Data Lifecycle Management

Along with meeting federal requirements such as FERPA, AWS recognizes that our education sector customers have to abide by state and local policies related to data retention and deletion. To facilitate capabilities to manage these requirements, AWS provides Object Lifecycle Management configurations.

Lifecycle configuration enables you to specify the lifecycle management of objects in a S3 bucket. The configuration is a set of one or more rules, where each rule defines an action for Amazon S3 to apply to a group of objects. These actions can be classified as follows:

- Transition actions – In which you define when objects transition to another storage class. For example, you may choose to transition objects to the STANDARD_IA (IA, for infrequent access) storage class 30 days after creation, or archive objects to the GLACIER storage class one year after creation.
- Expiration actions – In which you specify when the objects expire. Then Amazon S3 deletes the expired objects on your behalf.

By utilizing these rules, customers can define policies to manage their student data including transferring to economical long term storage options such as Amazon Glacier or securely delete required records.

Where Your Content is Stored in the USA

AWS data centers are built in clusters in various countries around the world. We refer to each of our data center clusters in a given country as a “Region”. You have access to numerous AWS Regions around the globe, and can choose to use one Region, all Regions or any combination of Regions.

Regions

AWS is continuously adding regions to serve our customers well. For the most updated map, please visit our global infrastructure page https://aws.amazon.com/about-aws/global-infrastructure/.

You retain complete control and ownership over the region in which your data is physically located, making it easy to meet regional compliance and data residency requirements. You can choose the AWS Region(s) where you would like to store your content, which is useful if you have specific geographic requirements. For example, if you are an US customer, you can choose to deploy your AWS services exclusively in the US East (Ohio) Region. If you make this choice, your content will be stored in the United States unless you select a different AWS Region.

Business Continuity

Business Continuity

Our infrastructure has a high level of availability and we provide you with the features you need to deploy a resilient IT architecture. Our systems are designed to tolerate system or hardware failures with minimal customer impact.

Disaster recovery is the process of preparing for and recovering from a disaster. Any event that has a negative impact on your business continuity or finances could be termed a disaster. The AWS Cloud supports many popular disaster recovery architectures, ranging from "pilot light" environments that are ready to scale up at a moment's notice to "hot standby" environments that enable rapid failover.

It is important to note that:

- All data centers are online and serving customers; no data center is "cold." In the case of a failure, automated processes move your data traffic away from the affected area.
- By distributing applications across multiple availability zones, you can remain resilient in the face of most failure modes, including natural disasters or system failures.
- You can build highly resilient systems in the cloud by employing multiple instances in multiple availability zones and using data replication to achieve extremely high recovery time and recovery point objectives.
- You are responsible for managing and testing the backup and recovery of your information system built on the AWS infrastructure. You can use the AWS infrastructure to enable faster disaster recovery of your critical IT systems without incurring the infrastructure expense of a second physical site.

For more information, visit **aws.amazon.com/disaster-recovery**.

Resources

Resources

Partners and Marketplace

APN Partner solutions enable automation and agility, scaling with your workloads, and you only pay for what you need and use. Easily find, buy, deploy, and manage these cloud-ready software solutions, including software as a service (SaaS) products, in a matter of minutes from the AWS Marketplace. These solutions work together to help secure your data in ways not possible on-premises, with solutions available for a wide range of workloads and use cases.

For more information, visit **aws.amazon.com/partners** and **aws.amazon.com/marketplace**.

Training

Whether you are just starting out, building on existing IT skills, or sharpening cloud knowledge, AWS Training can help you and your team advance your knowledge so you can be more effective using the cloud.

For more information, visit **aws.amazon.com/training**.

Quick Starts

Using our Quick Starts, you can follow best practices to begin your AWS security configuration setup, laying a solid foundation for meeting your global compliance requirements.

For more information, visit **aws.amazon.com/quickstart**.