SECURITY & COMPLIANCE QUICK REFERENCE GUIDE

2018


aws

NOTICES

This document is provided for informational purposes only. It represents AWS' 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' 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.

TABLE OF CONTENTS

OVERVIEW

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' requirements drive our portfolio of compliance reports, attestations, and certifications that enable our customers to run a secure and compliant cloud environment.

By using Amazon Web Services (AWS), you can achieve savings and scalability while still maintaining robust security and regulatory compliance.

"WE DETERMINED THAT SECURITY IN AWS IS SUPERIOR TO OUR ON-PREMISES DATA CENTER ACROSS SEVERAL DIMENSIONS, INCLUDING PATCHING, ENCRYPTION, AUDITING AND LOGGING, ENTITLEMENTS, AND COMPLIANCE."

John Brady
CISO, FINRA (Financial Industry Regulatory Authority)

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

We innovate rapidly at scale, continually incorporating your feedback into AWS services. This benefits you because our solutions improve over time, and we are constantly evolving our core security services such as identity and access management, logging and monitoring, encryption and key management, network segmentation, and standard DDoS protection.

You also get advanced security services designed by engineers with deep insight into global security trends, which allows your team to proactively address emerging risks in real time. This means you can choose the security that meets your needs as you grow, without upfront expenses and with much lower operational costs than if you manage your own infrastructure.

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

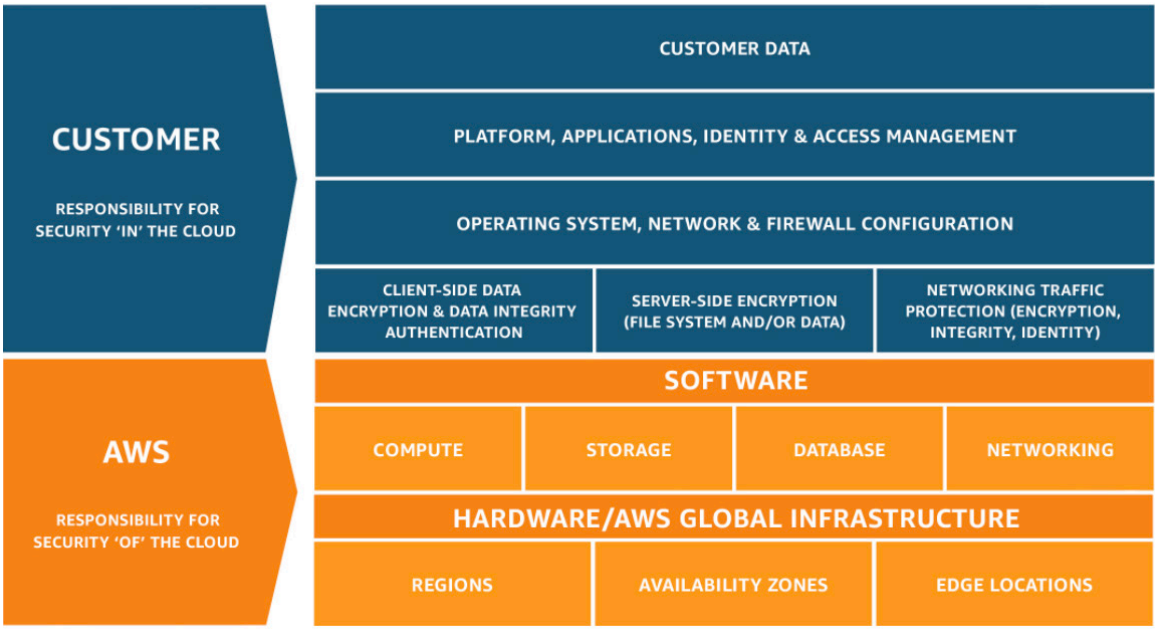
By using AWS, you get the benefit of the many security controls that we operate, thus reducing the number of security controls that you need to maintain. Your own compliance and certification programs are strengthened, while at the same time lowering your cost to maintain and run your specific security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

"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

HOW WE SHARE RESPONSIBILITY

SHARED RESPONSIBILITY MODEL



When you move your IT infrastructure to AWS, you adopt the model of shared responsibility shown to the left. This shared model reduces your operational burden because we operate, manage, and control the layers of IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. AWS is responsible for the security ***of*** the cloud, and as a customer you are responsible for security ***in*** the cloud.

Just as you share the responsibility for operating the IT environment with us, you also share the management, operation, and verification of IT controls.

AWS—SECURITY OF THE CLOUD

To help you get the most from the AWS security control framework, we have developed a security assurance program that uses best practices in global privacy and data protection.

To validate that we maintain a ubiquitous control environment that is operating effectively in our services and facilities across the globe, we seek third-party independent assessments. 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 environment. We monitor these industry groups to identify best practices that you can implement, and to better assist you with managing your control environment.


Rolling 24 Hour Call Monitor
4589 calls from 3447 vehicles

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 detailed information regarding the policies, processes, and controls we establish and operate. You can use this information to perform your control evaluation and verification procedures, as required under the applicable compliance standard.

You can incorporate the information that we provide about our risk and compliance program into your compliance framework. We use thousands of security controls to monitor that we maintain compliance with global standards and best practices. We provide you with 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 regulatory compliance.

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. AWS Config enables 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. You are also responsible for managing associated application software, as well as the configuration of the AWS-provided security group firewall. Your responsibilities vary depending on the AWS services you choose, how you integrate those services into your IT environment, and applicable laws and regulations.

In order to securely manage your AWS resources, you need to do the following three things:

- Know what resources you are using (asset inventory).
- Securely configure the guest OS and applications on your resources (secure configuration settings, patching, and anti-malware).
- Control changes to the resources (change management).

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 to meet your compliance requirements, while enabling users to quickly deploy the approved IT services they need.

Amazon GuardDuty

Amazon GuardDuty offers threat detection and continuous security monitoring for malicious or unauthorized behavior to help you protect your AWS accounts and workloads. The service monitors for activity that indicate a possible account compromise, potentially compromised instance, or reconnaissance by attackers.

ASSURANCE PROGRAMS

We categorize the AWS Assurance Programs into three categories: Certifications/Attestations, Laws/Regulations/Privacy, and Alignments/Frameworks.

Assurance Programs

Certifications/Attestations 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 are specific to your industry or function. We support you by providing security features and documents such as compliance playbooks, mapping documents, and whitepapers.

AWS' compliance with these laws, regulations, and programs is not formalized, either because certification is not available to cloud providers, or the certification is already covered by a larger umbrella within one of our formal certification/ attestation programs.

Global

CSA
Cloud Security Alliance Controls

ISO 9001
Global Quality Standard

ISO 27001
Security Management Controls

ISO 27017
Cloud Specific Controls

ISO 27018
Personal Data Protection

PCI DSS Level 1
Payment Card Standards

SOC 1
Audit Controls Report

SOC 2
Security, Availability, & Confidentiality Report

SOC 3
General Controls Report

United States

CJIS
Criminal Justice Information Services

DoD SRG
DoD Data Processing

FedRAMP
Government Data Standards

FERPA
Educational Privacy Act

FFIEC
Financial Institutions Regulation

FIPS
Government Security Standards

FISMA
Federal Information Security Management

GxP
Quality Guidelines and Regulations

HIPAA
Protected Health Information

ITAR
International Arms Regulations

MPAA
Protected Media Content

NIST
National Institute of Standards and Technology

SEC Rule 17a-4(f)
Financial Data Standards

VPAT / Section 508
Accessibility Standards

Asia Pacific

FISC [Japan]
Financial Industry Information Systems

IRAP [Australia]
Australian Security Standards

K-ISMS [Korea]
Korean Information Security

MTCS Tier 3 [Singapore]
Multi-Tier Cloud Security Standard

My Number Act [Japan]
Personal Information Protection

Europe

C5 [Germany]
Operational Security Attestation

Cyber Essentials Plus [UK]
Cyber Threat Protection

ENS High [Spain]
Spanish Government Standards

G-Cloud [UK]
UK Government Standards

IT-Grundschutz [Germany]
Baseline Protection Methodology

Our environments are continuously audited, and our infrastructure and services are approved to operate under several compliance standards and industry certifications across geographies and industries, including those shown below. 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, see the AWS Assurance Programs website.

PCI DSS

AWS is a Payment Card Industry Data Security Standard (PCI DSS) compliant service provider (since 2010), which 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 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 audit artifacts to demonstrate the security and compliance of your AWS infrastructure and services to your auditors or regulators.

Examples of audit artifacts include System and Organization Controls (SOC) and Payment Card Industry (PCI) reports.

ISO 27017

ISO 27017 provides guidance about the information security aspects of cloud computing, and recommends implementing cloud-specific information security controls that supplement the guidance of the ISO 27002 and ISO 27001 standards. This code of practice provides implementation guidance about information security controls that is specific to cloud service providers. AWS' attestation to the ISO 27017 guidance demonstrates our ongoing commitment to align with globally-recognized best practices, and also verifies that AWS has a system of highly precise controls in place that are specific to cloud services.

ISO 27018

ISO 27018 is a code of practice that focuses on protection of personal data in the cloud. It is based on the information security standard ISO 27002 and provides implementation guidance about ISO 27002 controls that are applicable to public cloud Personally Identifiable Information (PII). Alignment demonstrates to you that AWS has a system of controls in place, specifically addressing the privacy protection of your content.

SOC

AWS System and Organization Controls (SOC) Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives.

The purpose of these reports is to help you and your auditors understand the AWS controls established to support operations and compliance. There are three types of AWS SOC Reports:

- **SOC 1:** Provides information about AWS' control environment that may be relevant to your internal controls over financial reporting (ICFR), as well as information for assessment of the effectiveness of your ICFR.

- **SOC 2:** Provides you and service users with a business need with an independent assessment of AWS' control environment relevant to system security, availability, and confidentiality.

- **SOC 3:** Provides you and service users with a business need with an independent assessment of AWS' control environment and provides information about system security, availability, and confidentiality without disclosing AWS internal information.

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 Assessment Organization (3PAO), and maintain continuous monitoring requirements of FedRAMP.

DoD Cloud Security Model (CSM)
Standards for cloud computing issued by the U.S. Defense Information Systems Agency (DISA) and documented in the Department of Defense (DoD) Security Requirements Guide (SRG). Provides an authorization process for DoD workload owners who have unique architectural requirements because of their on DISA Impact Level (IL).

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 AWS environment to process, maintain, and store PHI.

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.

AWS CloudHSM

The AWS CloudHSM service allows you to protect your encryption keys within hardware security modules (HSMs) designed and validated to government standards for secure key management. You can securely generate, store, and manage the cryptographic keys used for data encryption such that they are accessible only by you.

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.

AWS gives 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 locations in which your data is physically stored, 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

Identity and Access Management (IAM) enables you to manage access to AWS services and resources securely. Using IAM, your administrators can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. Federation allows IAM roles to be mapped to permissions from central directory services.

Amazon Macie

Amazon Macie uses machine learning to automatically discover, classify, and protect sensitive data. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property, and continuously monitors data access activity for anomalies that might single unauthorized access or inadvertent data leaks.

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

We do not disclose your content, unless we are 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 disclosure.

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.

AWS Directory Service for Microsoft Active Directory

AWS Microsoft AD makes it easy to setup and run Microsoft Active Directory in the AWS cloud, or connect your AWS resources with an existing on-premises Microsoft Active Directory.

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 that CloudTrail provides to enable security analysis, resource change tracking, and compliance auditing.

AWS REGIONS

WHERE YOUR CONTENT IS STORED

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 an AWS Region. You have access to numerous AWS Regions around the globe, and can choose to use one AWS Region, all AWS Regions or any combination of AWS Regions.

You retain complete control over which AWS Region(s) your data is physically stored in, making it easy to meet your compliance and data residency requirements. For example, if you are a European customer, you can choose to deploy your AWS services exclusively in the EU (Frankfurt) Region. If you make this choice, your content will be exclusively stored in Germany unless you select a different AWS Region.

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.

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 AWS 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 AWS 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 that is 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***

AUTOMATION

Automating security tasks on AWS enables you to be more secure by reducing human configuration errors and giving your team more time to focus on other work that is critical to your business. Your security teams can use security automation and API integration to become more responsive and agile, making it easier to work closely with developer and operations teams to create and deploy code faster and more securely.

By automating infrastructure and application security checks whenever new code is deployed, you can continually enforce your security and compliance controls to help ensure confidentiality, integrity, and availability at all times. You can automate in a hybrid environment with our information management and security tools to easily integrate AWS as a seamless and secure extension of your on-premises and legacy environments.

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.

To help you get started quickly, Amazon Inspector includes a knowledge base of hundreds of rules that are mapped to common security best practices and vulnerability definitions. Examples of built-in rules include checking whether remote root login is enabled, or whether vulnerable software versions are installed. These rules are regularly updated by AWS security researchers.


SCUBA
SNORKEL
BENCH
TREND
COMP SET
BASELINE
ANALYSIS

RESOURCES

PARTNERS AND MARKETPLACE

AWS Partner Network (APN) 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 your cloud knowledge, AWS Training can help you and your team advance your understanding 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***


aws


aws