amazon web services

AWS SECURITY AND COMPLIANCE QUICK REFERENCE GUIDE

2017

OVERVIEW

OVERVIEW

When you migrate your regulated workloads to the cloud you gain access to our many governance-enabling features, which you can use to achieve a higher level of security at scale. Cloud-based governance offers a lower cost of entry, easier operations and improved agility by providing more oversight, security control, and central automation. Migrating to the cloud means that you will be able to leverage AWS to reduce the number of security controls that you need to maintain.

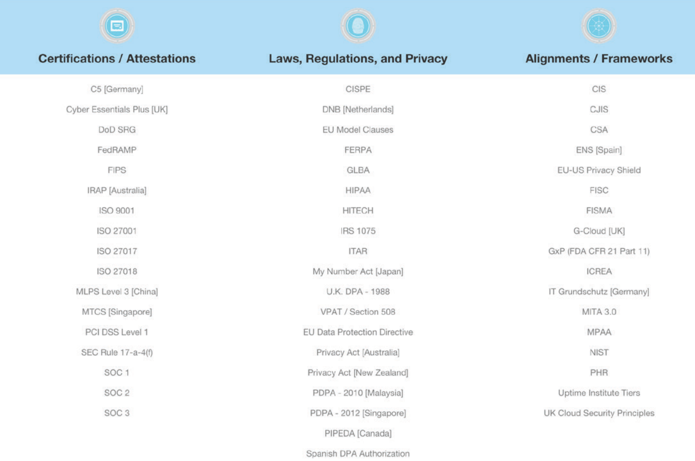
A compliant environment is the result of a properly secured environment. We provide a robust set of infrastructure controls that have been validated through numerous attestations and certifications. Each certification means that an auditor has verified that specific security controls are in place and operating as intended. You can learn more about all of the attestations and certifications that we support on the AWS Assurance Programs page.

We also provide a broad set of services and tools you can use to help achieve compliance in the cloud, including Amazon Inspector, AWS Artifact, AWS Service Catalog, AWS CloudTrail, AWS Config, and AWS Config Rules.

PROGRAMS

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.



Certifications / Attestations	Laws, Regulations, and Privacy	Alignments / Frameworks
C5 [Germany]	CISPE	CIS
Cyber Essentials Plus [UK]	DNB [Netherlands]	CJIS
DoD SRG	EU Model Clauses	CSA
FedRAMP	FERPA	ENS [Spain]
FIPS	GLBA	EU-US Privacy Shield
IRAP [Australia]	HIPAA	FISC
ISO 9001	HITECH	FISMA
ISO 27001	IRS 1075	G-Cloud [UK]
ISO 27017	ITAR	GxP (FDA CFR 21 Part 11)
ISO 27018	My Number Act [Japan]	ICREA
MLPS Level 3 [China]	U.K. DPA - 1988	IT Grundschutz [Germany]
MTCS [Singapore]	VPAT / Section 508	MITA 3.0
PCI DSS Level 1	EU Data Protection Directive	MPAA
SEC Rule 17-a-4(f)	Privacy Act [Australia]	NIST
SOC 1	Privacy Act [New Zealand]	PHR
SOC 2	PDPA - 2010 [Malaysia]	Uptime Institute Tiers
SOC 3	PDPA - 2012 [Singapore]	UK Cloud Security Principles
	PIPEDA [Canada]	
	Spanish DPA Authorization	

Figure 1: Assurance Programs

Note: We are continually adding programs. For the most current list of AWS Assurance Programs, visit the website.

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 functionality (such as security features) and enablers

PROGRAMS

(including compliance playbooks, mapping documents, and whitepapers). Formal "direct" certification of these laws, regulations and programs is either 1) not available to cloud providers or 2) represents a smaller subset of requirements already demonstrable by our current formal certification/ attestation programs.

Some of our most popular programs include:

PCI DSS - Payment Card Industry (PCI) Data Security Standards (DSS) are strict security standards for preventing fraud and protecting cardholder data for merchants that process credit card payments.

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.

SOC - AWS Service Organization Control (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 four types of AWS SOC Reports: AWS SOC 1 Report, AWS SOC 2: Security & Availability Report, AWS SOC 2: Confidentiality Report, and AWS SOC 3: Security & Availability Report.

FedRAMP – A U.S. government program for ensuring standards in security assessment, authorization, and continuous monitoring. FedRAMP follows the NIST 800-53 security control standards.

PROGRAMS

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 depending on impact level.

HIPAA – The Health Insurance Portability and Accountability Act (HIPAA) contains strict security and compliance standards for organizations processing or storing Protected Health Information (PHI).

You can find complete descriptions of each program that we align to on the AWS Assurance Programs webpage.

AWS Artifact

The AWS Artifact portal 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 Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals that validate the implementation and operating effectiveness of AWS security controls.

You can access the AWS Artifact portal directly from the AWS Management Console.

INDUSTRIES

INDUSTRIES

Customers in the following industries are using AWS to meet their regulatory compliance needs:

- Agriculture and Mining
- Analytics and Big Data
- Computers and Electronics
- E-commerce
- Education
- Energy and Utilities
- Financial Services
- Food and Beverage
- Gaming
- Government
- Healthcare and Life Sciences
- Insurance
- Manufacturing
- Media and Entertainment
- Non-Profit Organization
- Real Estate and Construction
- Retail, Wholesale, and Distribution
- Software and Internet
- Telecommunications
- Transportation and Logistics
- Travel and Hospitality

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 in Figure 2. 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 relieves the operational burden on you.

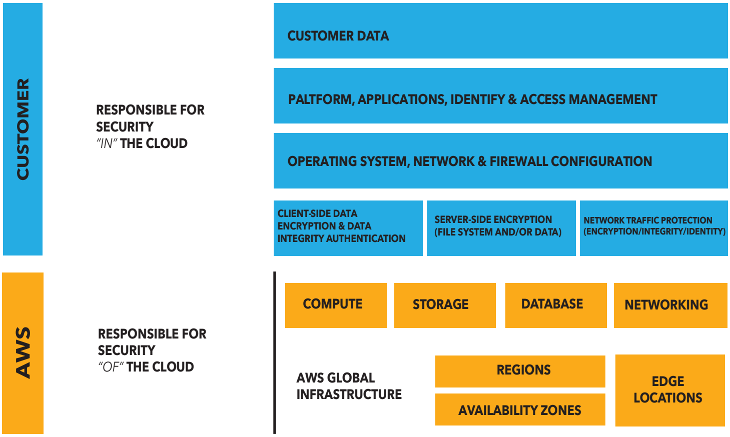

CUSTOMER
RESPONSIBLE FOR SECURITY "IN" THE CLOUD
CUSTOMER DATA
PALTFORM, APPLICATIONS, IDENTIFY & ACCESS MANAGEMENT
OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION
CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION
SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)
NETWORK TRAFFIC PROTECTION (ENCRYPTION/INTEGRITY/IDENTITY)
AWS
RESPONSIBLE FOR SECURITY "OF" THE CLOUD
COMPUTE
STORAGE
DATABASE
NETWORKING
AWS GLOBAL INFRASTRUCTURE
REGIONS
AVAILABILITY ZONES
EDGE LOCATIONS

Figure 2: Shared Responsibility Model

The shared responsibility model also extends to IT controls. 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.

You can leverage the AWS control and compliance documentation to perform your control evaluation and verification procedures, as required under the applicable compliance standard.

AWS - COMPLIANCE OF THE CLOUD

We are responsible for helping you maintain a secure and compliance-ready environment. In general, 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 can implement, and to better assist you with managing their control environment.

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.

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

CUSTOMER - COMPLIANCE IN THE CLOUD

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

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

YOUR CONTENT

YOUR CONTENT

By design, we give you ownership and control over your content. Using simple, but powerful tools, you can determine where your content will be stored, secure your content in transit or at rest, and manage your user's access to AWS services and resources.

> **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.

Access – Using our advanced set of access, encryption, and logging features (such as AWS CloudTrail), you can manage access to your content and AWS services and resources. We do not access or use your content for any purpose other than as legally required and for maintaining the AWS services and providing them to you and your end users.

Storage – You choose the region(s) that you want to store your content in. We will not move or replicate your content outside of the customer's chosen region(s), except as legally required and as necessary to maintain the AWS services and provide them to you and your end users. For example, if you are a European customer, you can choose to deploy your AWS services exclusively in the EU (Germany) Region.

YOUR CONTENT

Security – You choose how your content is secured. We offer you strong encryption for your content in transit or at rest, and we provide you with the option to manage your own encryption keys.

Disclosure of your content – 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.

Security Assurance – 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.

> **Note**: To validate that we manage security of the cloud with technical and physical controls designed to prevent unauthorized access to or disclosure of customer content, an independent auditor has certified that we confirm alignment with industry standards.

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 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.

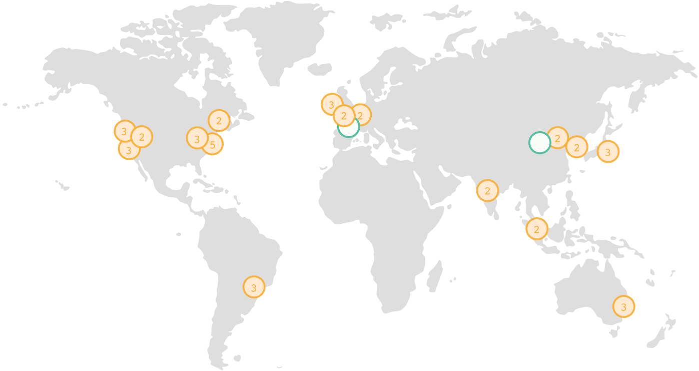


Figure 3: Regions

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 a European customer, you can choose to deploy your AWS services exclusively in the EU (Germany) Region. If you make this choice, your content will be 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.

> **Resilience** is about reducing the likelihood of assets becoming unavailable.
>
> **Recovery** is about reducing the impact of when assets become unavailable.
>
> **Backup** is a strategy for dealing with the loss of data whether accidental or intentional.

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.

To learn more about Disaster Recovery on AWS, see **https://aws.amazon.com/disaster-recovery/**.

Our data centers are built in clusters in various global regions. All data centers are online and serving customers; no data center is "cold." In the case of a failure, automated processes move customer data traffic away from the affected area.

We provide you with the flexibility to place instances and store data within multiple geographic regions, as well as across multiple availability zones within each region. By distributing applications across multiple availability zones, you can remain resilient in the face of most failure modes, including natural disasters or system failures.

BUSINESS CONTINUITY

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. The AWS cloud supports many popular disaster recovery architectures from “pilot light” environments that are ready to scale up at a moment’s notice to “hot standby” environments that enable rapid failover.

SECURITY

SECURITY

Cloud security at AWS is our highest priority. The AWS Security Center provides you with security and compliance details about AWS.

We operate the global cloud infrastructure that you use to provision a variety of basic computing resources such as processing and storage. Our global infrastructure includes the facilities, network, hardware, and operational software (e.g., host OS, virtualization software, etc.) that support the provisioning and use of these resources. Our global infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. As an AWS customer, you can be assured that you're building web architectures on top of one of the most secure computing infrastructures in the world.

RESOURCES

RESOURCES

You can access all of the webpages and whitepapers referenced within this document at the AWS Security and Compliance Quick Reference Resource Hub at **https://aws.amazon.com/compliance/reference/**.

PARTNERS AND MARKETPLACE

The AWS Partner Network (APN) is the global partner program for AWS. It helps APN Partners build successful AWS-based businesses or solutions by providing business, technical, marketing, and go-to-market support. For more information, visit **https://aws.amazon.com/partners/**.

AWS Marketplace is a sales channel that makes it easy for AWS Sellers to offer software solutions that run on the AWS cloud. For more information, visit **https://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 **https://aws.amazon.com/training/**.

amazon
web services