Amazon Web Services: Risk and Compliance

November 2020

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

AWS serves a variety of customers, including those in regulated industries. Through our shared responsibility model, we enable customers to manage risk effectively and efficiently in the IT environment, and provide assurance of effective risk management through our compliance with established, widely recognized, frameworks, and programs. This paper outlines the mechanisms that AWS has implemented to manage risk on the AWS side of the Shared Responsibility Model, and the tools that customers can leverage to gain assurance that these mechanisms are being implemented effectively.

Introduction

AWS and its customers share control over the IT environment. Therefore, security is a shared responsibility. When it comes to managing security and compliance in the AWS Cloud, each party has distinct responsibilities. A customer's responsibility depends on which services they are using. However, in general, customers are responsible for building their IT environment in a manner that aligns with their specific security and compliance requirements.

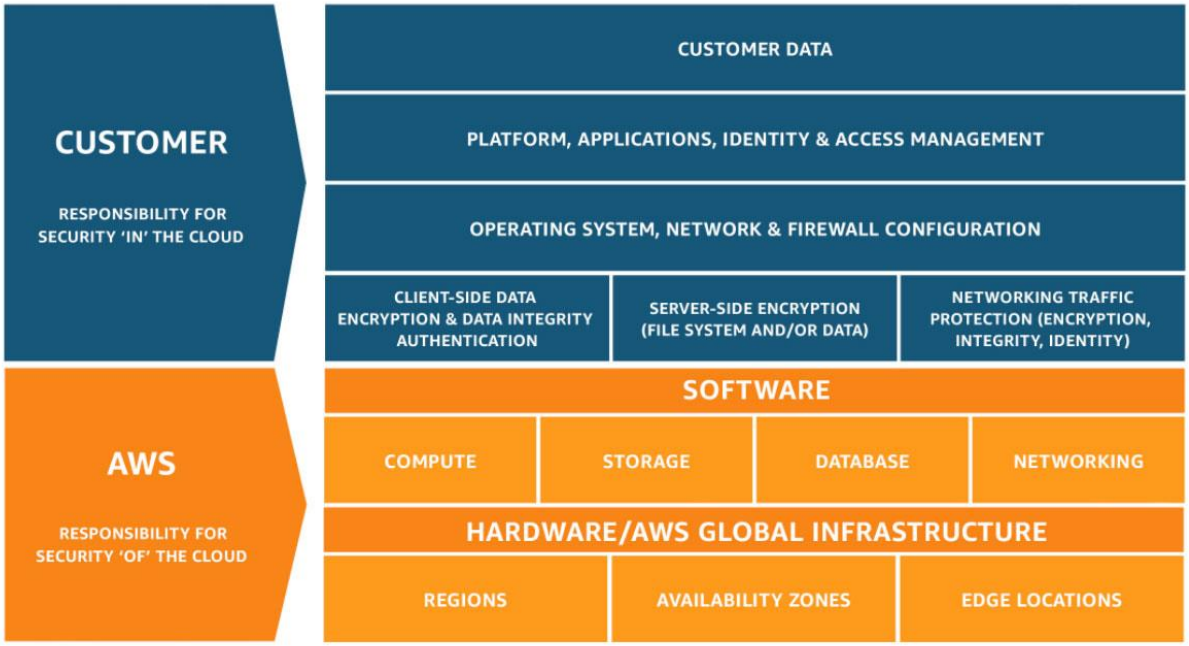
This paper provides more details about each party's security responsibilities and the ways customers can benefit from the AWS Risk and Compliance Program.

Shared responsibility model

Security and compliance are shared responsibilities between AWS and the customer. Depending on the services deployed, this shared model can help relieve the customer's operational burden. This is because AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches) and other associated application software, in addition to the configuration of the AWS-provided security group firewall.

We recommend that customers carefully consider the services they choose because their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. It is possible for customers to enhance their security and/or meet their more stringent compliance requirements by leveraging technology such as host-based firewalls, host-based intrusion detection and prevention, encryption, and key management.

The nature of this shared responsibility also provides the flexibility and customer control that permits customers to deploy solutions that meet industry-specific certification requirements.



This shared responsibility model also extends to IT controls. Just as the responsibility to operate the IT environment is shared between AWS and its customers, the management, operation, and verification of IT controls is also a shared responsibility. AWS can help customers by managing those controls associated with the physical infrastructure deployed in the AWS environment. Customers can then use the AWS control and compliance documentation available to them to perform their control evaluation and verification procedures as required. For examples of how responsibility for certain controls is shared between AWS and its customers, see the AWS Shared Responsibility Model.

Evaluating and integrating AWS controls

AWS provides a wide range of information about its IT control environment to customers through technical papers, reports, certifications, and other third-party attestations. This documentation helps customers to understand the controls in place, relevant to the AWS services they use, and how those controls have been validated. This information also helps customers account for and validate that controls in their extended IT environment are operating effectively.

Traditionally, internal and/or external auditors validate the design and operational effectiveness of controls by process walkthroughs and evidence evaluation. This type of

direct observation and verification, by the customer or customer's external auditor, is generally performed to validate controls in traditional on-premises deployments.

In the case where service providers are used (such as AWS), customers can request and evaluate third-party attestations and certifications. These attestations and certifications can help assure the customer of the design and operating effectiveness of control objective and controls validated by a qualified, independent third party. As a result, although some controls might be managed by AWS, the control environment can still be a unified framework where customers can account for and verify that controls are operating effectively and accelerating the compliance review process.

Third-party attestations and certifications of AWS provide customers with visibility and independent validation of the control environment. Such attestations and certifications may help relieve customers of the requirement to perform certain validation work themselves for their IT environment in the AWS Cloud.

AWS risk and compliance program

AWS has integrated a risk and compliance program throughout the organization. This program aims to manage risk in all phases of service design and deployment and continually improve and reassess the organization's risk-related activities. The components of the AWS integrated risk and compliance program are discussed in greater detail in the following sections.

AWS business risk management

AWS has a business risk management (BRM) program that partners with AWS business units to provide the AWS Board of Directors and AWS senior leadership a holistic view of key risks across AWS. The BRM program demonstrates independent risk oversight over AWS functions. Specifically, the BRM program does the following:

- Performs risk assessments and risk monitoring of key AWS functional areas
- Identifies and drives remediation of risks
- Maintains a register of known risks

To drive the remediation of risks, the BRM program reports the results of its efforts, and escalates where necessary, to directors and vice presidents across the business to inform business decision-making.

Operational and business management

AWS uses a combination of weekly, monthly, and quarterly meetings and reports to, among other things, ensure communication of risks across all components of the risk management process. In addition, AWS implements an escalation process to provide management visibility into high priority risks across the organization. These efforts, taken together, help ensure that risk is managed consistently with the complexity of the AWS business model.

In addition, through a cascading responsibility structure, vice presidents (business owners) are responsible for the oversight of their business. To this end, AWS conducts weekly meetings to review operational metrics and identify key trends and risks before they impact the business.

Executive and senior leadership play important roles in establishing the AWS tone and core values. Every employee is provided with the company's Code of Business Conduct and Ethics, and employees complete periodic training. Compliance audits are performed so that employees understand and follow established policies.

The AWS organizational structure provides a framework for planning, executing, and controlling business operations. The organizational structure includes roles and responsibilities to provide for adequate staffing, efficiency of operations, and the segregation of duties. Management has also established appropriate lines of reporting for key personnel. The company's hiring verification processes include validation of education, previous employment, and, in some cases, background checks as permitted by law and regulation for employees commensurate with the employee's position and level of access to AWS facilities. The company follows a structured on-boarding process to familiarize new employees with Amazon tools, processes, systems, policies, and procedures.

Control environment and automation

AWS implements security controls as a foundational element to manage risk across the organization. The AWS control environment is comprised of the standards, processes, and structures that provide the basis for implementing a minimum set of security requirements across AWS.

While processes and standards included as part of the AWS control environment stand on their own, AWS also leverages aspects of Amazon's overall control environment. Leveraged tools include:

- Tools used across all Amazon businesses, such as the tool that manages separation of duties
- Certain Amazon-wide business functions, such as legal, human resources, and finance

In instances where AWS leverages Amazon's overall control environment, the standards and processes governing these mechanisms are tailored specifically for the AWS business. This means that the expectations for their use and application within the AWS control environment may differ from the expectations for their use and application within the overall Amazon environment. The AWS control environment ultimately acts as the foundation for the secure delivery of AWS service offerings.

Control automation is a way for AWS to reduce human intervention in certain recurring processes comprising the AWS control environment. It is key to effective information security control implementation and associated management of risks. Control automation seeks to proactively minimize potential inconsistencies in process execution that might arise due to the flawed nature of humans conducting a repetitive process. Through control automation, potential process deviations are eliminated. This provides increased levels of assurance that a control will be applied as designed.

Engineering teams at AWS across security functions are responsible for engineering the AWS control environment to support increased levels of control automation wherever possible. Examples of automated controls at AWS include:

- **Governance and Oversight:** Policy versioning and approval
- **Personnel Management:** Automated training delivery, rapid employee termination
- **Development and Configuration Management:** Code deployment pipelines, code scanning, code backup, integrated deployment testing
- **Identity and Access Management:** Automated segregation of duties, access reviews, permissions management
- **Monitoring and Logging:** Automated log collection and correlation, alarming
- **Physical Security:** Automated processes related to AWS data centers, including hardware management, data center security training, access alarming, and physical access management
- **Scanning and Patch Management:** Automated vulnerability scanning, patch management, and deployment

Controls assessment and continuous monitoring

AWS implements a variety of activities prior to and after service deployment to further reduce risk within the AWS environment. These activities integrate security and compliance requirements during the design and development of each AWS service and then validate that services are operating securely after they are moved into production (launched).

Risk management and compliance activities include two pre-launch activities and two post-launch activities. The pre-launch activities are:

- AWS Application Security risk management review to validate that security risks have been identified and mitigated
- Architecture readiness review to help customers ensure alignment with compliance regimes

At the time of its deployment, a service will have gone through rigorous assessments against detailed security requirements to meet the AWS high bar for security. The post-launch activities are:

- AWS Application Security ongoing review to help ensure service security posture is maintained
- Ongoing vulnerability management scanning

These control assessments and continuous monitoring allow regulated customers the ability to confidently build compliant solutions on AWS services. For a list of services in the scope for various compliance programs see the AWS Services in Scope webpage.

AWS certifications, programs, reports, and third-party attestations

AWS regularly undergoes independent third-party attestation audits to provide assurance that control activities are operating as intended. More specifically, AWS is audited against a variety of global and regional security frameworks dependent on region and industry. AWS participates in over 50 different audit programs.

The results of these audits are documented by the assessing body and made available for all AWS customers through AWS Artifact. AWS Artifact is a no cost self-service portal for on-demand access to AWS compliance reports. When new reports are

released, they are made available in AWS Artifact, allowing customers to continuously monitor the security and compliance of AWS with immediate access to new reports.

Depending on a country's or industry's local regulatory or contractual requirements, AWS may also undergo audits directly with customers or governmental auditors. These audits provide additional oversight of the AWS control environment to ensure that customers have the tools to help themselves operate confidently, compliantly, and in a risk-based manner using AWS services.

For more detailed information about the AWS certification programs, reports, and third-party attestations, visit the AWS Compliance Program webpage. You can also visit the AWS Services in Scope webpage for service-specific information.

Cloud Security Alliance

AWS participates in the voluntary Cloud Security Alliance (CSA) Security, Trust & Assurance Registry (STAR) Self-Assessment to document its compliance with CSA-published best practices. The CSA is "the world's leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment"[1]. The CSA Consensus Assessments Initiative Questionnaire (CAIQ) provides a set of questions the CSA anticipates a cloud customer and/or a cloud auditor would ask of a cloud provider. It provides a series of security, control, and process questions, which can then be used for a wide range of efforts, including cloud provider selection and security evaluation.

There are two resources available to customers that document the alignment of AWS to the CSA CAIQ. The first is the CSA CAIQ Whitepaper, and the second is a more detailed control mapping to our SOC-2 controls which is available to via AWS Artifact. For more information about the AWS participation in CSA CAIQ, see the AWS CSA site.

Customer cloud compliance governance

AWS customers are responsible for maintaining adequate governance over their entire IT control environment, regardless of how or where IT is deployed. Leading practices include:

- Understanding the required compliance objectives and requirements (from relevant sources)
- Establishing a control environment that meets those objectives and requirements

- Understanding the validation required based on the organization's risk tolerance
- Verifying the operating effectiveness of their control environment

Deployment in the AWS Cloud gives enterprises different options to apply various types of controls and various verification methods.

Strong customer compliance and governance may include the following basic approach:

1. Reviewing the AWS Shared Responsibility Model, AWS Security Documentation, AWS compliance reports, and other information available from AWS, together with other customer-specific documentation. Try to understand as much of the entire IT environment as possible, and then document all compliance requirements into a comprehensive cloud control framework.
2. Designing and implementing control objectives to meet the enterprise compliance requirements as laid out in the AWS Shared Responsibility Model.
3. Identifying and documenting controls owned by outside parties.
4. Verifying that all control objectives are met and all key controls are designed and operating effectively.

Approaching compliance governance in this manner will help customers gain a better understanding of their control environment and will help clearly delineate the verification activities to be performed.

Conclusion

Providing highly secure and resilient infrastructure and services to our customers is a top priority for AWS. Our commitment to our customers is focused on working to continuously earn customer trust and ensure customers maintain confidence in operating their workloads securely on AWS. To achieve this, AWS has integrated risk and compliance mechanisms that include:

- The implementation of a wide array of security controls and automated tools
- Continuous monitoring and assessment of security controls to help ensure AWS operational effectiveness and strict adherence to compliance regimes
- Independent risk assessment by the AWS Business Risk Management program
- Operational and business management mechanisms

In addition, AWS regularly undergoes independent third-party audits to provide assurance that the control activities are operating as intended. These audits, along with the many certifications AWS has obtained, provide an additional level of validation of the AWS control environment that benefit customers.

Taken together with customer-managed security controls, these efforts allow AWS to securely innovate on behalf of customers and help customers improve their security posture when building on AWS.

Contributors

Contributors to this document include:

- Marta Taggart, Senior Program Manager, AWS Security
- Bradley Roach, Risk Manager, AWS Business Risk Management
- Patrick Woods, Senior Security Specialist, AWS Security

Further reading

AWS provides customers with information regarding its security and control environment by:

- Obtaining and maintaining industry certifications and independent third-party attestations as listed on the AWS Compliance Program Page.
- Consistently publishing information about the AWS security and control practices in whitepapers and web content, like the AWS Security Blog.
- Providing in-depth descriptions of how AWS utilizes automation at scale to manage our service infrastructure in The AWS Builders Library.
- Enhancing transparency by providing compliance certificates, reports, and other documentation directly to AWS customers via the self-service portal known as AWS Artifact.
- Providing AWS Compliance Resources and consistently documenting and publishing answers to queries on AWS Compliance FAQs webpage.
- Customers can follow the design principles in the AWS Well-Architected Framework for guidance of how to approach the above the line configuration of their workloads build on AWS.

Document revisions

Date	Description
November 2020	This version includes substantial changes that include removing the reference information about compliance programs and schemes because this information is available on the AWS Compliance Programs and AWS Services in Scope by Compliance Program webpages. Additionally, we removed the section covering common compliance questions because that information is now available on the AWS Compliance FAQs webpage.
May 2011	First publication

Notes

[1] https://cloudsecurityalliance.org/about/