AWS Shared Responsibility

PROVIDED BY ALIGNED TECHNOLOGY GROUP

Applying the AWS Shared Responsibility Model in Practice

Once a customer understands the AWS Shared Responsibility Model and how it generally applies to operating in the cloud, they must determine how it applies to their use case. Customer responsibility varies based on many factors, including the AWS services and Regions they choose, the integration of those services into their IT environment, and the laws and regulations applicable to their organization and workload.

The following exercises can help customers in determining the distribution of responsibility based on specific use case:

- **External / Internal**
- **Digital Transformation**
- **Security Capabilities**
- **Objectives**
- **Third-Party Audit**
- **Internal / External Audit**
- **Workload Optimization**
- **Software Acquisition**
- **Consulting Partnership**

ALIGNED TECHNOLOGY GROUP

Aligned Technology Group (Aligned), is a specialized technology advisor and consultant focused on specific areas of excellence, including: Cloud, Data, Security and Core Infrastructure. The firm provides professional services to large and mid-sized enterprise-class organizations throughout the United States. Aligned is a value-centric partner with a differentiated engagement approach dedicated to selecting and employing technologies to enable and empower business success. With a team of highly experienced consultants and technologists and an expansive partner ecosystem, Aligned is attuned to the latest in technology advancements, innovations and industry trends.

919.825.3614

alignedtg.com

aws PARTNER Advanced Tier Services

External / Internal

Determine external and internal security and related compliance requirements and objectives, and consider industry frameworks like the NIST Cybersecurity Framework (CSF) and ISO.

Security Capabilities

Review the security functionality and configuration options of individual AWS services within the security chapters of AWS service documentation.

Third-Party Audit

Review third-party audit attestation documents to determine inherited controls and what required controls may be remaining for you to implement in your environment.

Workload Optimization

Perform a Well-Architected Review of your AWS workloads to evaluate the implementation of best practices for security, reliability, and performance.

Consulting Partnership

Explore AWS Security Competency Partners offering expertise and proven customer success securing every stage of cloud adoption, from initial migration through ongoing day-to-day management.

Digital Transformation

Consider employing the AWS Cloud Adoption Framework (CAF) and Well-Architected best practices to plan and execute your digital transformation at scale.

Objectives

Evaluate the AWS Security, Identity, and Compliance services to understand how they can be used to help meet your security and compliance objectives.

Internal / External Audit

Provide your internal and external audit teams with cloud-specific learning opportunities by leveraging the Cloud Audit Academy training programs.

Software Acquisition

Explore solutions available in the AWS Marketplace digital catalog with thousands of software listings from independent software vendors that enable you to find, test, buy, and deploy software that runs on AWS.