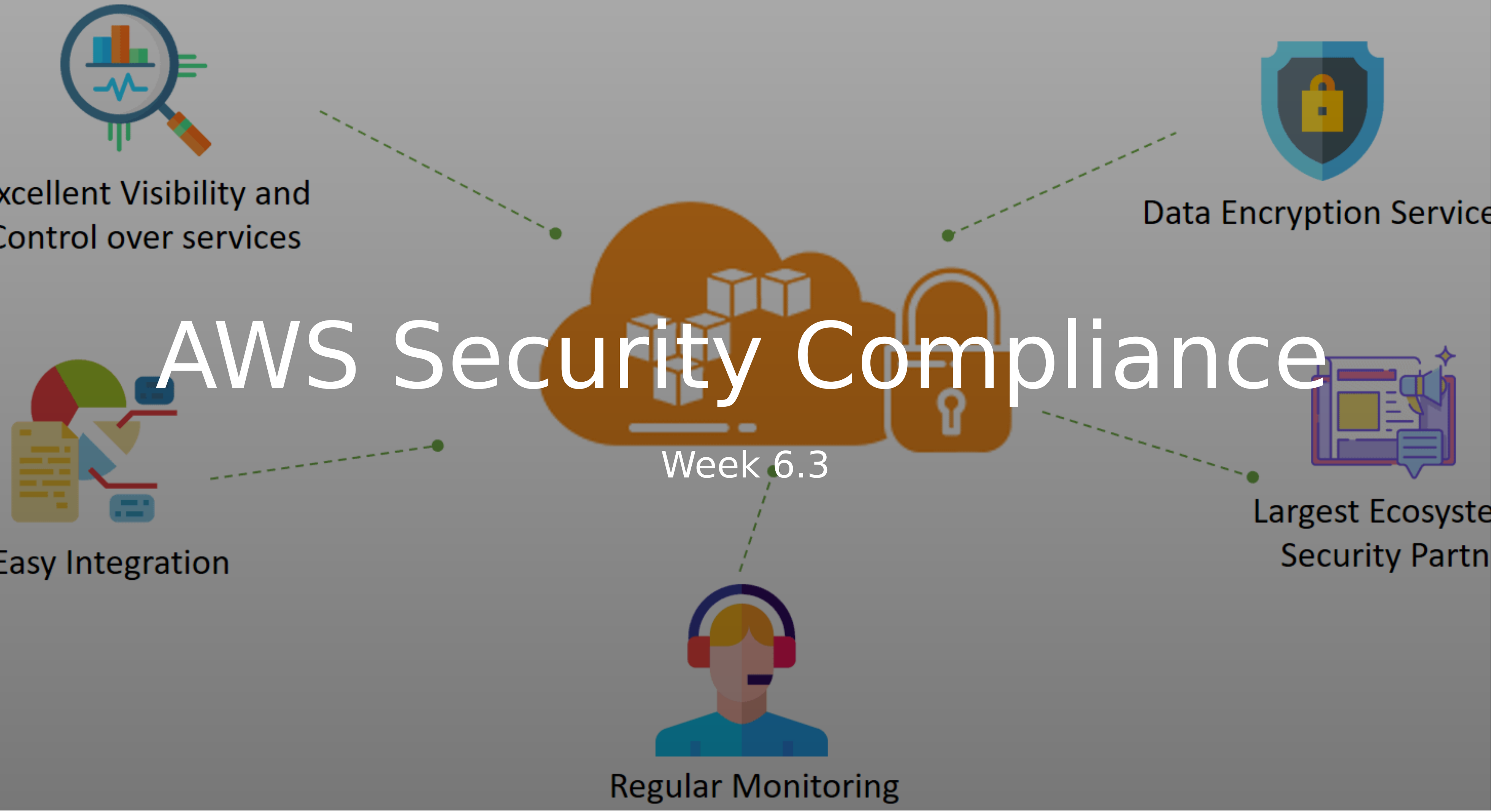
AWS Security Compliance

Week 6.3



What you will Learn

- The AWS compliance approach, which includes assurance programs
- AWS risk and compliance programs, such as risk management, control environment, and information security
- AWS customer compliance responsibilities

AWS Compliance Approach

- As described in the shared responsibility model for security, AWS and its customers share control over the IT environment.
- This means that both parties are responsible for managing the IT environment.
- In this model, AWS responsibility includes providing services in a highly secure controlled environment and an array of security features for customers to use.
- The customer’s responsibility includes configuring their IT environments in a secure and controlled manner for their purposes.

AWS Security Information

- AWS communicates information about its relevant security and control environment to customers.
- AWS provides security information in the following ways:
- Obtains industry certifications and independent third-party attestations.
- Publishes information about the AWS security and control practices in technical papers and website content.
- Provides certificates, reports, and other documentation directly to AWS customers under nondisclosure agreements (NDAs), as required.

AWS Assurance Programs

- AWS engages with external certifying bodies and independent auditors to provide customers with information about the policies, processes, and controls established and operated by AWS:
- **Certifications and attestations** – Compliance certifications and attestations are assessed by a third-party, independent auditor. They result in a certification, audit report, or attestation of compliance.
- **Laws, regulations, and privacy** – AWS customers remain responsible for complying with applicable compliance laws and regulations. In some cases, AWS offers functionality to support customer compliance. Examples of this functionality include security features, enablers, and legal agreements, such as the AWS Data Processing Agreement and the Business Associate Addendum.
- **Industry alignments and frameworks** – Compliance alignments and frameworks include published security or compliance requirements for a specific purpose, such as specific industries or functions. AWS provides functionality, such as security features, and also offers compliance playbooks, mapping documents, and technical papers for these types of pr

AWS Risk and Compliance Program

- AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework.
- This information can assist customers in documenting a complete control and governance framework that has AWS included as an important part of that framework.
- The AWS risk and compliance program are made up of three components:
  - Business risk management
  - Control environment and automation
  - Information security

AWS Risk Management

- AWS management develops a strategic business plan that includes risk identification and the implementation of controls to mitigate or manage risks.
- AWS management re-evaluates the strategic business plan at least biannually.
- This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks.
- In addition, the AWS control environment is subject to various internal and external risk assessments.
- The AWS compliance and security team establishes an information security framework and policies that are based on the following governing bodies:
  - Control Objectives for Information and related Technology (COBIT)
  - American Institute of Certified Public Accountants (AICPA)
  - National Institute of Standards and Technology (NIST)

AWS Risk Management

- AWS maintains the security policy and performs application security reviews.
- These reviews assess the confidentiality, integrity, and availability of data, in addition to conformance to the information security (IS) policy.
- AWS security regularly scans for vulnerabilities on all public service endpoint IP addresses.
- However, scans are not performed on customer Amazon Elastic Compute Cloud (Amazon EC2) instance interfaces.
- AWS security notifies the appropriate parties to remediate any identified vulnerabilities.
- In addition, external vulnerability threat assessments are performed regularly by independent security firms.

AWS Control Environment

- AWS manages a comprehensive control environment that includes policies, processes, and control activities that use various aspects of the Amazon overall control environment.
- This controlled environment is in place for the secure delivery of AWS service offerings.
- The collective control environment encompasses the **people**, **processes**, and **technology** necessary to support the operating effectiveness of the AWS control framework.
- AWS integrates applicable cloud-specific controls identified by leading cloud computing industry bodies into the AWS control framework.
- AWS continues to monitor these industry groups for ideas about which leading practices can be implemented.
- AWS monitors the groups to assist customers with managing their control environment.

Information Security

- AWS has a formal information security program designed to protect the confidentiality, integrity, and availability of customers’ systems and data.
- AWS publishes a security technical paper that addresses how AWS helps customers secure their data.
- For more information, refer to AWS Security.

Customer Compliance Requirements

- AWS customers must maintain adequate governance over the entire IT control environment regardless of how IT is deployed.
- Leading practices include an understanding of required compliance objectives and requirements (from relevant sources), and establishing a controlled environment that meets those objectives and requirements.
- These practices also include an understanding of the validation required based on the organization's risk tolerance and 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.
- By staying engaged in the compliance and governance process with AWS, customers can ensure that compliance requirements are being met.

Customer Compliance Requirements

- Strong customer compliance and governance might include the following basic approach:
- Review AWS information together with other information to understand as much of the entire IT environment as possible. Then, document all compliance requirements.
- Design and implement control objectives to meet the enterprise compliance requirements.
- Identify and document controls owned by outside parties.
- Verify that all control objectives are met and all key controls are designed and operating effectively.

Key Takeaways

- AWS Cloud compliance enables customers to understand the robust controls in place at AWS to maintain security and data protection in the cloud.
- Customers operate in an environment that is controlled by AWS security. Because customer systems are built on top of the AWS Cloud infrastructure, compliance responsibilities are shared.
- AWS supports many security standards and compliance certifications. These standards and certifications help customers satisfy compliance requirements for virtually every regulatory agency around the world