Welcome to AWS Security Compliance Program.

This lesson explores the following topics:

- 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

AWS responsibility

- Provide highly secure and controlled environment.
- Provide an array of security features.

Customer responsibility:

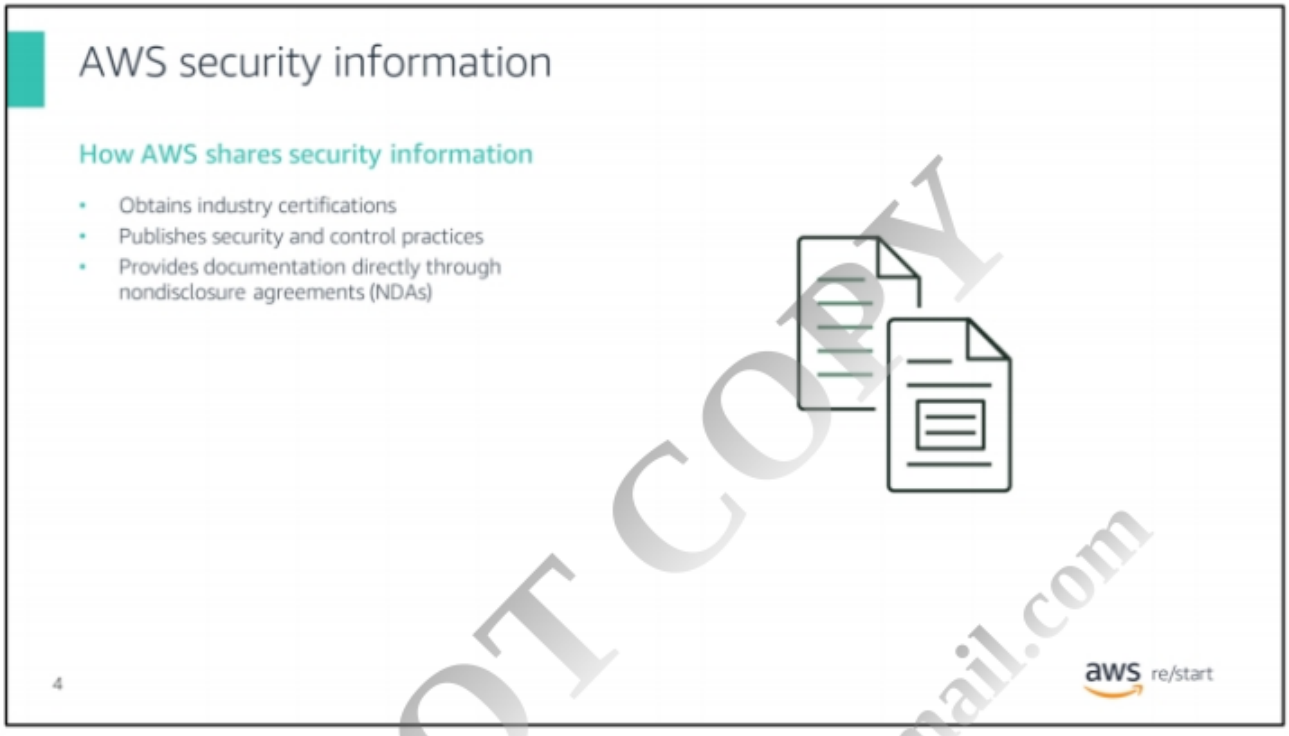
- Configure IT.

3

aws re/start

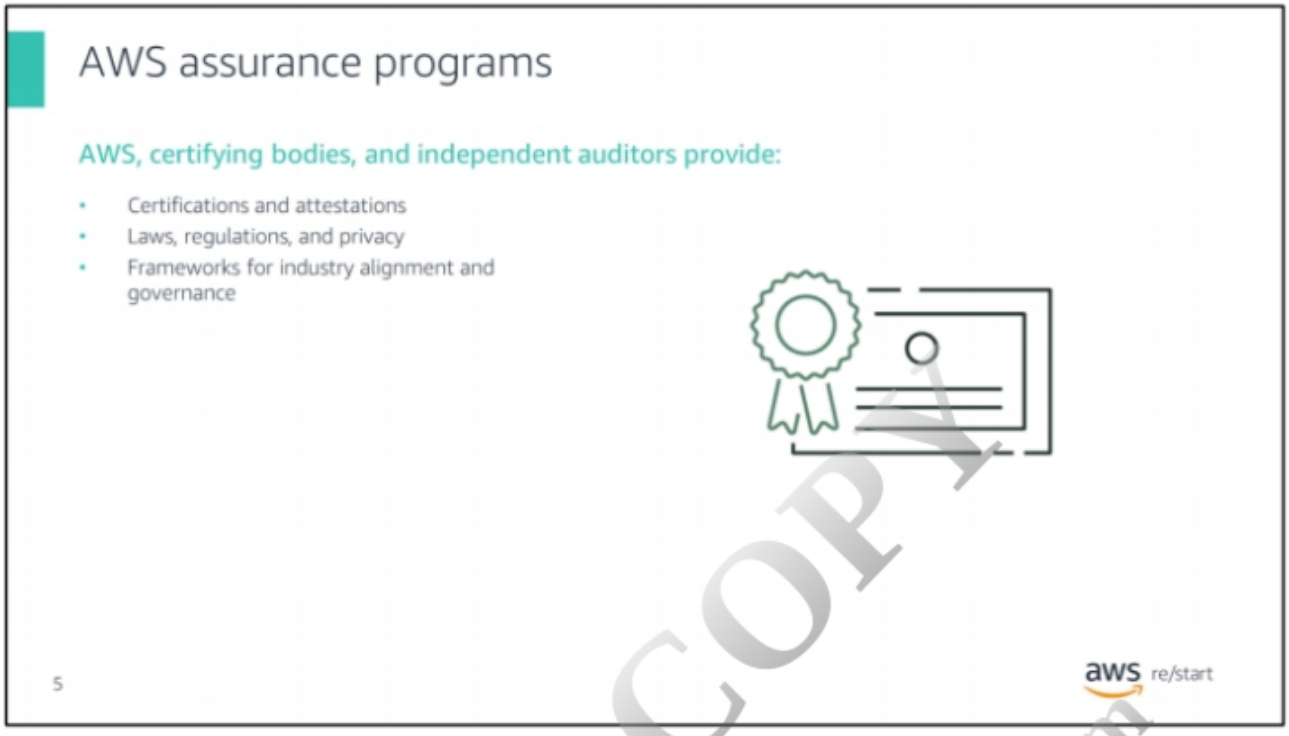
As described in the shared responsibility model for security, AWS and its customers share control over the IT environment. This means that both parties are responsible for managing the IT environment. In this model, AWS responsibility includes providing services in a highly secure controlled environment 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 communicates information about its relevant security and control environment to customers. AWS provides security information through the following ways:

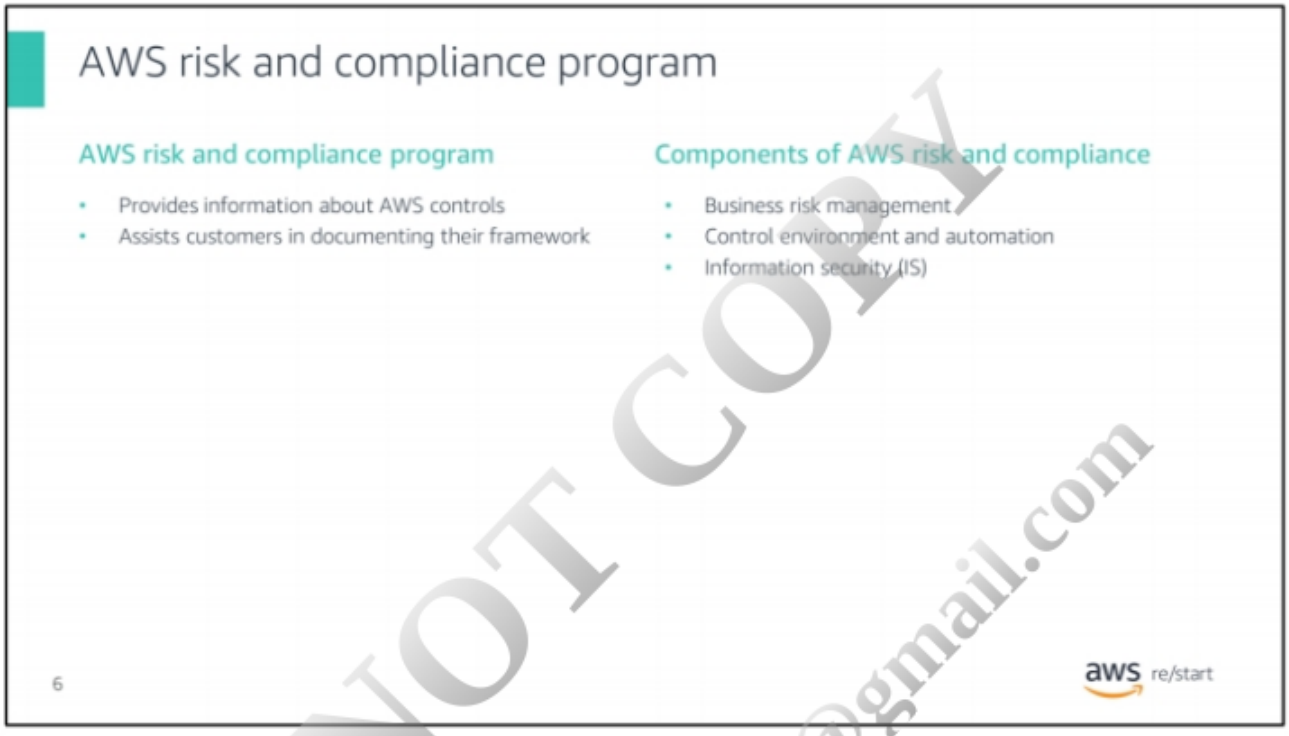
- Obtains industry certifications and independent third-party attestations.
- Publishes information about the AWS security and control practices in technical papers and website content.
- Provides certificates, reports, and other documentation directly to AWS customers under nondisclosure agreements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



AWS 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, regulation, 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 a specific industry or function. AWS provides functionality, such as security features, and also offers compliance

playbooks, mapping documents, and technical papers for these types of programs.

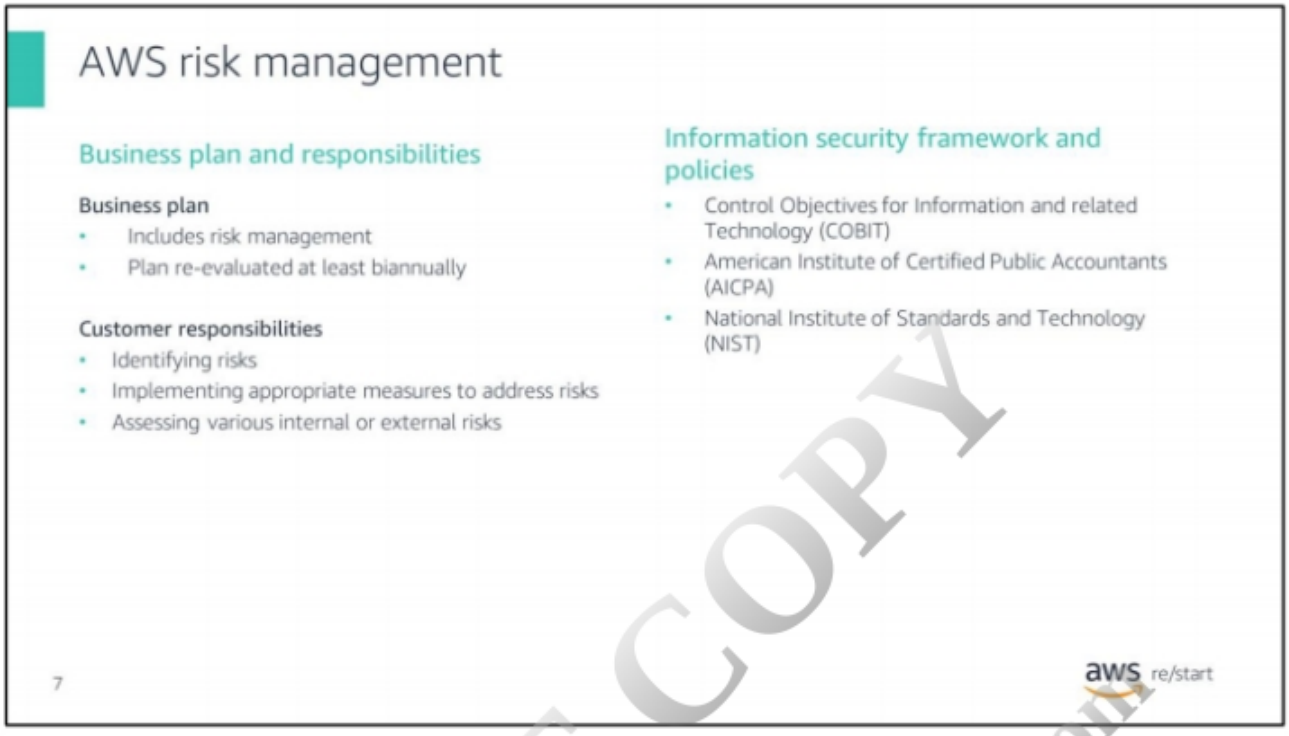


AWS provides information about its risk and compliance program to enable customers to incorporate AWS controls into their governance framework. This information can assist customers in documenting a complete control and governance framework that has AWS included as an important part of that framework.

The AWS risk and compliance program is made up of three components:

- Business risk management
- Control environment and automation
- Information security

The next topics explores each of the AWS risk and compliance programs in more detail.

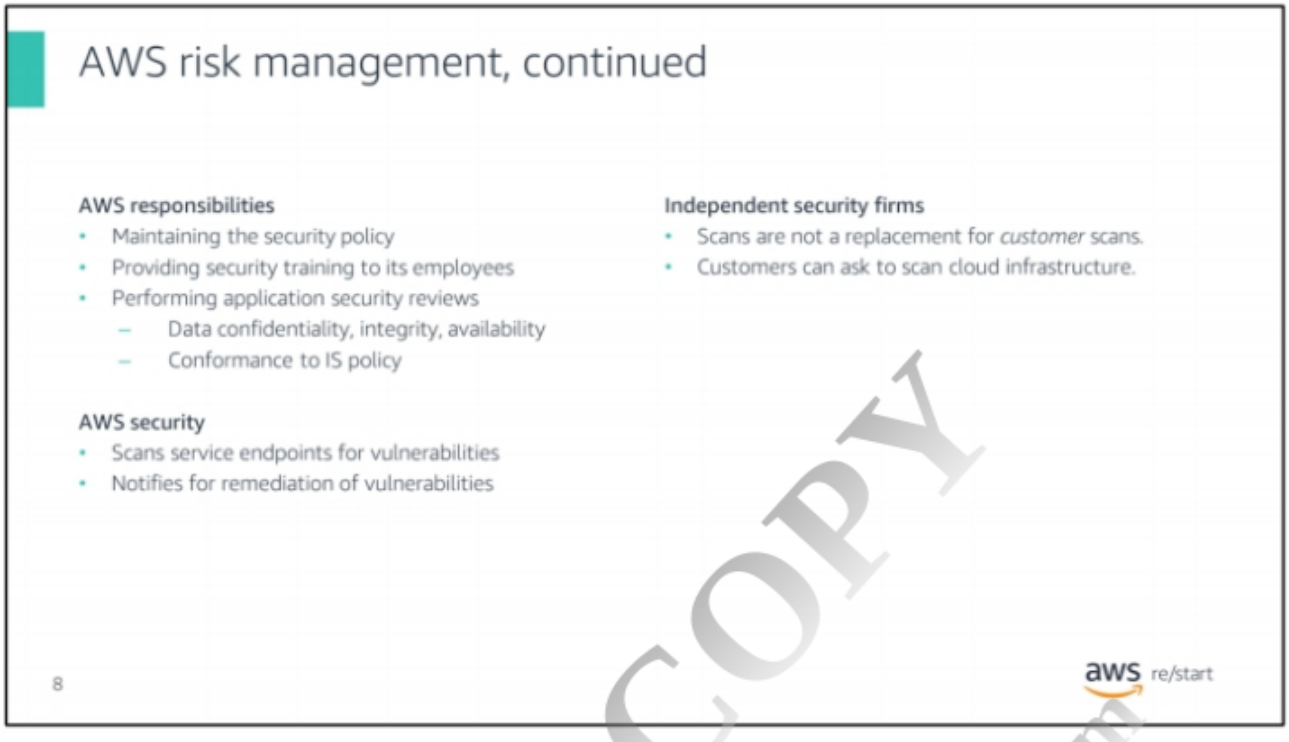


AWS management develops a strategic business plan that includes risk identification and the implementation of controls to mitigate or manage risks. AWS management re-evaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility 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 maintains the security policy, provides security training to its employees, 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

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.

Independent security firms

In addition, external vulnerability threat assessments are performed regularly by independent security firms. Findings and recommendations resulting from these assessments are categorized and delivered to AWS leadership. These scans are done to validate the health and viability of the underlying AWS infrastructure. They are not meant to replace the customer's own vulnerability scans required to meet their specific compliance requirements. Customers can request permission to conduct scans of their cloud infrastructure as long as

they are limited to the customer's instances and do not violate the AWS acceptable use policy.