Module 6. Cloud Security and Compliance

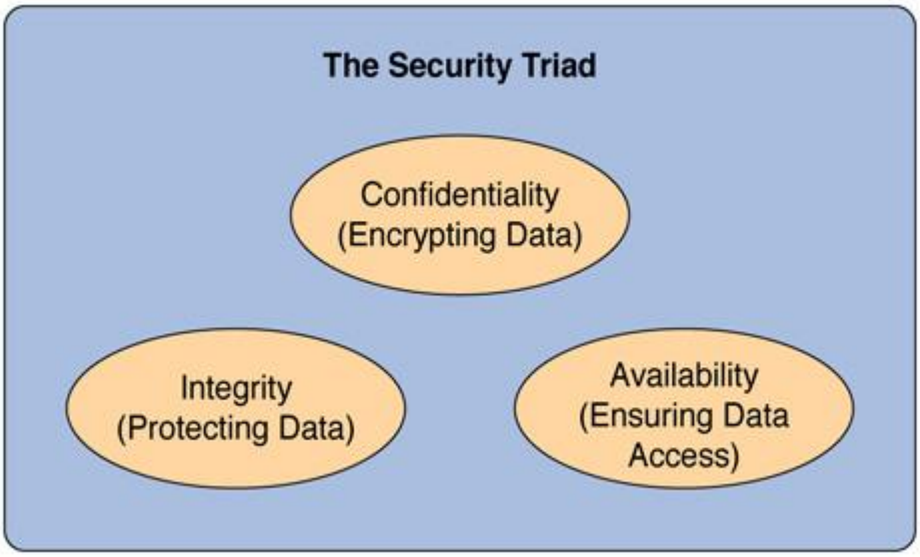
This module covers the following subjects:

- **An Introduction to AWS Security**: This section discusses the significant aspects of AWS's approaches to securing infrastructure and resources.
- **AWS Security Compliance Programs**: This section of the module ensures that you understand the many efforts that AWS engages in to ensure that you can maintain security compliance with any laws and regulations you might face.

You must understand Amazon's approaches to security when it comes to AWS. It is also important to know specifics regarding the levels of compliance and attestation that AWS believes are important. This module discusses these points in detail, providing specific technologies that AWS uses to help ensure you can create the most secure architecture possible in the cloud and beyond.

AN INTRODUCTION TO AWS SECURITY

Amazon understands that security is a genuine concern for many organisations considering a move to public (or hybrid) clouds. As a result, they have incredible built-in levels of protection for your organisation. This security includes massive efforts around *confidentiality*, *integrity*, and *availability* (CIA) and is known as the "security triad" depicted in Figure 6-1.


The Security Triad
Confidentiality (Encrypting Data)
Integrity (Protecting Data)
Availability (Ensuring Data Access)

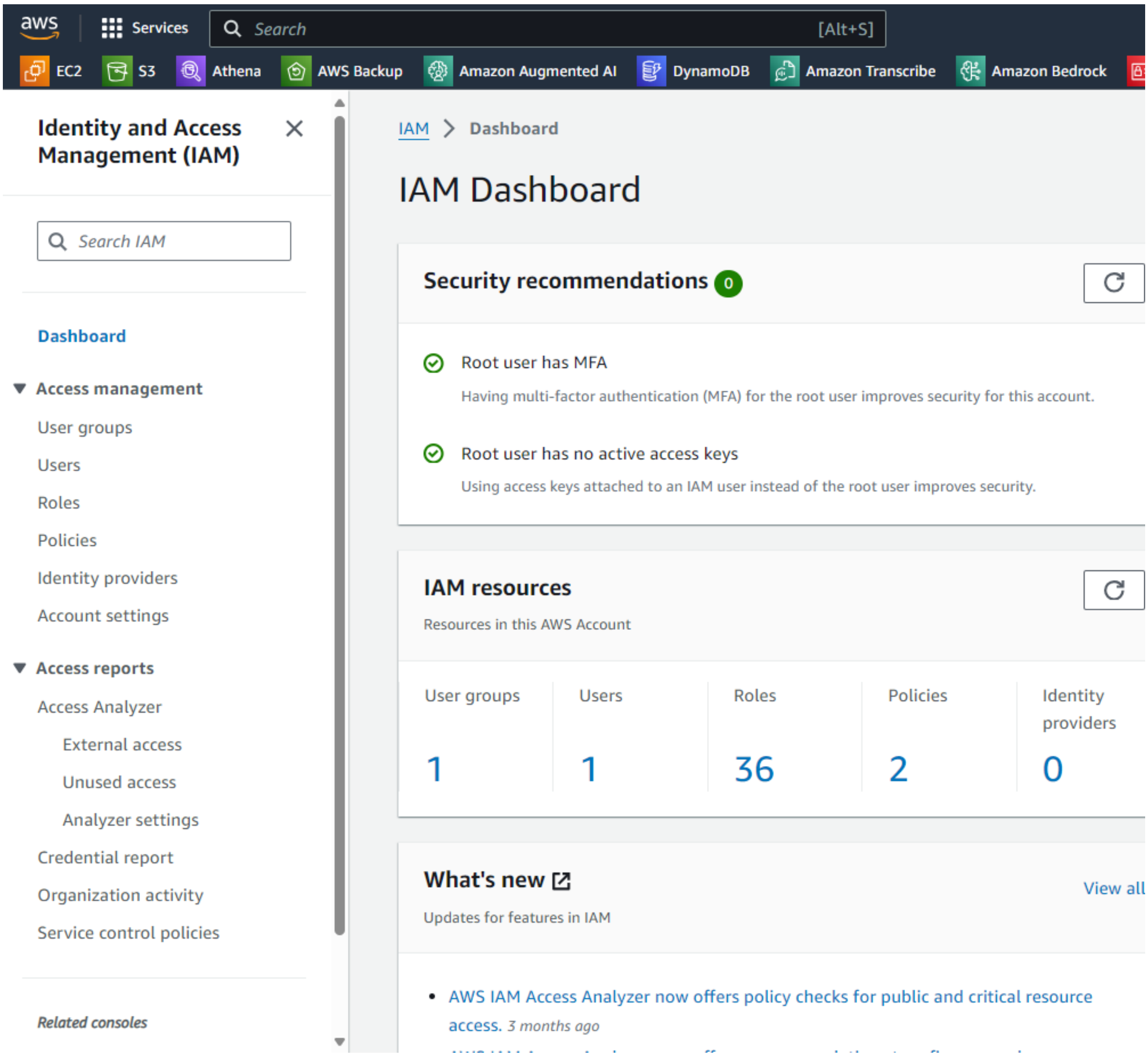
nd

Figure 6-1 The Security Triad

What are some of the main approaches that Amazon takes to secure AWS? Let's cover those now.

The first is keeping customer data as safe as possible. Amazon ensures a resilient and highly available infrastructure, and it uses strong security technologies and safeguards for its security responsibilities.

With AWS, you can take advantage of rapid innovations in security technology at scale. Including a robust identity and access management (IAM) system, data encryption at rest and in transit, and segmentation services. Figure 6-2 shows the IAM components in AWS.



aws Services Search [Alt+S]

EC2 S3 Athena AWS Backup Amazon Augmented AI DynamoDB Amazon Transcribe Amazon Bedrock

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

▼ Access reports

Access Analyzer

External access

Unused access

Analyzer settings

Credential report

Organization activity

Service control policies

Related consoles

IAM > Dashboard

IAM Dashboard

Security recommendations 0

✓ Root user has MFA

Having multi-factor authentication (MFA) for the root user improves security for this account.

✓ Root user has no active access keys

Using access keys attached to an IAM user instead of the root user improves security.

IAM resources

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	1	36	2	0

What's new

View all

Updates for features in IAM

- AWS IAM Access Analyzer now offers policy checks for public and critical resource access. *3 months ago*

Figure 6-2 IAM in AWS

With AWS security, you pay for what you need. This system permits high levels of security with controlled and elastic capacity and costs.

AWS also ensures diverse compliance support to offer adherence to governance, oversight, and automation.

Also, AWS follows a shared responsibility model that divides responsibility (clearly) between the customer (you) and Amazon. You can leverage their incredible expertise in secure infrastructures and technology knowledge. However, you must have expertise in securing components within AWS services. For example, you would be responsible for patching some virtual machine (EC2) deployments.

Note

Note: Amazon keeps the hardware on which your virtual machines reside highly secure.

Specific security products and features encompass a variety of tools and monitoring resources, including the following:

- **Robust network security**: Built-in firewalling, encryption in transit, private connectivity options, and built-in DDoS mitigation.
- **Efficient security tools**: Management of resource commissions and decommissions, inventory and configuration management tools, and best practice template definitions.
- **Data encryption at every level**: This includes database systems, key management, hardware-based storage options, and API support (like everything in AWS).
- **Access control and management**: Identity and Access Management, multifactor authentication, federation support, integrations of IAM into all services, and API support.
- **Monitoring and logging tools**: Deep visibility into API calls, log aggregation tools, alerts, and reduced risks.
- **AWS Marketplace**: Anti-malware, intrusion prevention systems (IPSs), and policy management tools.

AWS SECURITY COMPLIANCE PROGRAMS

How does Amazon measure their success regarding compliance with security best practices and regulations? The success of their many customers! Customers drive AWS efforts in these categories (to name just a few):

- Compliance reports
- Attestations
- Certifications

Compliance programs and adherence to them will help you implement excellent security at scale in AWS. This should also help you realise cost savings overall.

Amazon, especially once you are a customer, will communicate its security responsibilities, successes, failures, and overall efforts using the following means:

- Obtaining industry certifications
- Obtaining independent, third-party attestations
- Publishing security information whitepapers and web content
- Providing certificates, reports, and other documents to customers, sometimes under a nondisclosure agreement (NDA)

Amazon also provides the following to customers:

- Functionality through security features
- Compliance playbooks
- Mapping documents

AWS also offers a robust risk and compliance program that helps you with the following:

- Risk management
- Control environments
- Information security

Amazon regularly scans all public-facing points for vulnerabilities. They will even use independent, third-party firms to perform threat assessments against their technologies and infrastructure. If you (as a customer) are interested in performing penetration (pen) testing against your resources, you may do so, but you must obtain explicit permission from AWS.

Remember, as a customer of AWS, you should (must):

- Engage in a robust security lifecycle approach that includes a review phase, a design phase, and then phases of identification and verification. The identification phase should include external controls that are required to secure the customer resources.
- Understand the required compliance objectives.
- Establish a control environment.
- Understand the validation based on risk tolerances.
- Consistently verify the effectiveness of the security measures deployed.

For more information about AWS and security compliance, visit the AWS compliance home page at

https://aws.amazon.com/compliance.

This page links to a wealth of valuable resources.

EXAM PREPARATION TASKS

- **REVIEW ALL TOPICS**

- **DEFINE ALL KEY TERMS AND CHECK ANSWERS IN THE GLOSSARY.**

- **DO THE QUIZ – REPEAT UNTIL YOU PASS IT (100% PASSMARK).**

DEFINE KEY TERMS

Define the following key terms from this module and check your answers in the Glossary:

Confidentiality

integrity

availability

compliance

Q&A

1. Why might you turn to the AWS Marketplace when working on your security infrastructure in AWS?

2. What should you do if you are interested in penetration testing your AWS data and resources?