AWS Security Governance at Scale – Intensive Training («AWSE07»)

Learn how to facilitate developer speed and agility, and incorporate preventive and detective controls.
By the end of this course, you will be able to apply governance best practices.

Duration: 1 day
Price: 900.–
Course documents: Digital original AWS courseware

Content

Security is foundational to AWS. Governance at scale is a new concept for automating cloud governance that can help companies retire manual processes in account management, budget enforcement, and security and compliance. By automating common challenges, companies can scale without inhibiting agility, speed, or innovation. In addition, they can provide decision makers with the visibility, control, and governance necessary to protect sensitive data and systems.

Course Introduction

- Instructor introduction
- Learning objectives
- Course structure and objectives
- Course logistics and agenda

Module 1: Governance at Scale

- Governance at scale focal points
- Business and Technical Challenges

Module 2: Governance Automation

- Multi-account strategies, guidance, and architecture
- Environments for agility and governance at scale
- Governance with AWS Control Tower
- Use cases for governance at scale

Module 3: Preventive Controls

- Enterprise environment challenges for developers
- AWS Service Catalog
- Resource creation
- Workflows for provisioning accounts
- Preventive cost and security governance
- Self-service with existing IT service management (ITSM) tools
- **Lab 1: Deploy Resources for AWS Catalog**
  - Create a new AWS Service Catalog portfolio and product
  - Add an IAM role to a launch constraint to limit the actions the product can perform
  - Grant access for an IAM role to view the catalog items
  - Deploy an S3 bucket from an AWS Service Catalog product

Module 4: Detective Controls

- Operations aspect of governance at scale
- Resource monitoring

- Configuration rules for auditing
- Operational insights
- Remediation
- Clean up accounts
- **Lab 2: Compliance and Security Automation with AWS Config**
  - Apply Managed Rules through AWS Config to selected resources
  - Automate remediation based on AWS Config rules
  - Investigate the Amazon Config dashboard and verify resources and rule compliance
- **Lab 3: Taking Action with AWS Systems Manager**
  - Setup Resource Groups for various resources based on common requirements
  - Perform automated actions against targeted Resource Groups

Module 5: Resources

- Explore additional resources for security governance at scale

Key Learnings

- Establishing a landing zone with AWS Control Tower
- Configuring AWS Organizations to create a multi-account environment
- Implementing identity management using AWS Single Sign-On users and groups
- Federating access using AWS SSO
- Enforcing policies using prepackaged guardrails
- Centralizing logging using AWS CloudTrail and AWS Config
- Enabling cross-account security audits using AWS Identity and Access Management (IAM)
- Defining workflows for provisioning accounts using AWS Service Catalog and AWS Security Hub

Target audience

This course is intended for the following job roles:

- Solution Architect
- Cyber Security

Why should you attend this specific course? What are my benefits from taking this course? The **Voice of the Instructor answers these questions**. We have asked our instructor team to write a short text about WHY this course is very relevant for the respective job roles and what you can expect from attending the course. You can find this section in the course description under the «*Additional Information*» section.

Requirements

We recommend that attendees of this course have attended the following course (or equivalent knowledge):

- AWS Security Essentials – Intensive Training («AWSE04»)

Additional information

Voice of the Instructor

Participating in the "AWS Security Governance at Scale" course can provide several benefits for individuals and organizations. Here are some reasons why you should consider participating:

1. Advanced Security Governance Knowledge: The course focuses on security governance specifically within the AWS environment. It goes beyond basic security practices and delves into the intricacies of establishing robust governance frameworks. You will learn about developing

and implementing security policies, defining roles and responsibilities, establishing security baselines, and enforcing compliance across your AWS infrastructure. This advanced knowledge will help you effectively govern security in large-scale AWS deployments.

2. Scalable Security Solutions: As organizations scale their AWS environments, managing security becomes increasingly complex. The course will equip you with strategies and techniques to effectively govern security at scale. You'll learn about automation, security orchestration, and using AWS-native services like AWS Config, AWS CloudFormation, AWS Organizations, and AWS Identity and Access Management (IAM) to implement and enforce security policies consistently across multiple AWS accounts and resources.

3. Risk Management and Compliance: Security governance plays a vital role in managing risk and maintaining compliance. The course will cover risk assessment methodologies, identifying and prioritizing security risks, and implementing controls to mitigate those risks effectively. You'll gain insights into compliance frameworks and how to align your AWS security governance with relevant regulations and industry standards. This knowledge will help you ensure your organization's security posture, protect sensitive data, and meet compliance requirements.

4. Streamlined Security Operations: The course will guide you on streamlining security operations within a large-scale AWS environment. You'll learn about security monitoring and incident response, leveraging AWS services like AWS CloudTrail, AWS Config, AWS Security Hub, and AWS GuardDuty. By integrating these services into your security governance framework, you can enhance threat detection, automate incident response, and efficiently manage security events and incidents.

5. Collaboration and Communication: As security governance often involves multiple stakeholders, the course will emphasize effective collaboration and communication. You'll learn how to engage with different teams, such as developers, operations, and management, to foster a security-aware culture and ensure security practices are understood and followed. Effective communication and collaboration can help drive a shared responsibility for security across your organization.

6. Career Advancement: The knowledge and skills gained from the "AWS Security Governance at Scale" course can significantly enhance your professional profile. AWS certifications and expertise in security governance are highly valued in the industry. By participating in the course, you'll have the opportunity to demonstrate your proficiency in designing and implementing security governance frameworks at scale, opening doors to career advancement in cloud security, AWS architecture, or security management roles.

Overall, the "AWS Security Governance at Scale" course will provide you with the necessary knowledge and skills to govern security effectively within large-scale AWS environments. It will enable you to establish robust security governance frameworks, manage risks, maintain compliance, streamline security operations, and drive collaboration across your organization.

Further courses

- Migrating to AWS – Intensive Training («AWSM01»)
- Running Containers on Amazon Elastic Kubernetes Service (Amazon EKS) – Intensive Training («AWSA09»)
- AWS Cloud Financial Management for Builders – Intensive Training («AWSA08»)

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-it-provider/amazon-web-services-aws/aws-cyber-security/course-aws-security-governance-at-scale-intensive-training