

**AWS Security Governance at Scale**

**Course Number:** AWS-172  
**Duration:** 1 day

**Overview**

This AWS Security Governance at Scale training course teaches attendees how to automate their cloud governance so that they can retire manual processes. Participants learn how to provide decision-makers with the visibility, control, and governance rules necessary to protect sensitive data and systems.

Accelebrate is an AWS Training Partner (ATP) and this hands-on official AWS Classroom Training course is taught by an accredited Amazon Authorized Instructor (AAI).

**Prerequisites**

All students should have taken the official AWS free, self-paced digital course [AWS Security Fundamentals](https://explore.skillbuilder.aws/learn/course/external/view/elearning/48/aws-security-fundamentals-second-edition) (2 hours) and [AWS Security Essentials](file:////training/aws-security-essentials) classroom training.

**Materials**

All AWS Security training attendees receive comprehensive courseware.

**Software Needed on Each Student PC**

A modern web browser and an Internet connection that allows connections by SSH or Remote Desktop (RDP) into AWS virtual machines.

**Objectives**

* Establish a landing zone with AWS Control Tower
* Configure AWS Organizations to create a multi-account environment
* Implement identity management using AWS Single Sign-On users and groups
* Federate access using AWS SSO
* Enforce policies using prepackaged guardrails
* Centralize logging using AWS CloudTrail and AWS Config
* Enable cross-account security audits using AWS Identity and Access Management (IAM)
* Define workflows for provisioning accounts using AWS Service Catalog and AWS Security Hub

**Outline**

* Introduction
* Governance at Scale
  + Governance at scale focal points
  + Business and Technical Challenges
* 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
* 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
  + 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.
* Detective Controls
  + Operations aspect of governance at scale
  + Resource monitoring
  + Configuration rules for auditing
  + Operational insights
  + Remediation
  + Clean up accounts
  + 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
  + Taking Action with AWS Systems Manager
  + Setup Resource Groups for various resources based on common requirements
  + Perform automated actions against targeted Resource Groups
* Conclusion and Resources
  + Explore additional resources for security governance at scale