



---

## Security Engineering on AWS

**Duration: 3 Days**    **Course Code: GK3338**

---

### Overview:

Security Operations on AWS demonstrates how to efficiently use AWS security services to stay secure and compliant in the AWS cloud. The course focuses on the AWS-recommended security best practices that you can implement to enhance the security of your data and systems in the cloud. The course highlights the security features of AWS key services including compute, storage, networking, and database services. This course also refers to the common security control objectives and regulatory compliance standards and examines use cases for running regulated workloads on AWS across different verticals, globally. You will also learn how to leverage AWS services and tools for automation and continuous monitoring—taking your security operations to the next level.

---

### Target Audience:

This course is intended for: Security engineers, Security architects, Security analysts, Security auditors, Individuals who are responsible for governing, auditing, and testing an organization's IT infrastructure, and ensuring conformity of the infrastructure to security, risk, and compliance guidelines

---

### Objectives:

- This course teaches you how to:
    - Manage and audit your AWS resources from a security perspective.
  - Assimilate and leverage the AWS shared security responsibility model.
    - Monitor and log access and usage of AWS compute, storage, networking, and database services.
  - Manage user identity and access management in the AWS cloud.
    - Assimilate and leverage the AWS shared compliance responsibility model.
  - Use AWS security services such as AWS Identity and Access Management, Amazon Virtual Private Cloud, AWS Config, AWS CloudTrail, AWS Key Management Service, AWS CloudHSM, and AWS Trusted Advisor.
    - Identify AWS services and tools to help automate, monitor, and manage security operations on AWS.
  - Implement better security controls for your resources in the AWS cloud.
    - Perform security incident management in the AWS cloud.
- 

### Prerequisites:

We recommend that attendees of this course have the following prerequisites:

- Attended AWS Security Fundamentals
  - Experience with governance, risk, and compliance regulations and control objectives
  - Working knowledge of IT security practices
  - Working knowledge of IT infrastructure concepts
-

## Content:

This course covers the following concepts:

Identity and Access Management

Using AWS Security Services

Day 1

- Introduction to Cloud Security
- Security of the AWS Cloud
- Cloud Aware Governance and Compliance

Day 2

- Securing AWS Infrastructure Services
- Securing AWS Container Services
- Securing AWS Abstracted Services

Day 3

- Data Protection in the AWS Cloud
- Building Compliant Workloads on AWS—Case Study
- Security Incident Management in the Cloud

---

## Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

[training@globalknowledge.qa](mailto:training@globalknowledge.qa)

[www.globalknowledge.com/en-qa/](http://www.globalknowledge.com/en-qa/)

Global Knowledge, Qatar Financial Center, Burj Doha, Level 21, P.O.Box 27110, West Bay, Doha, Qatar