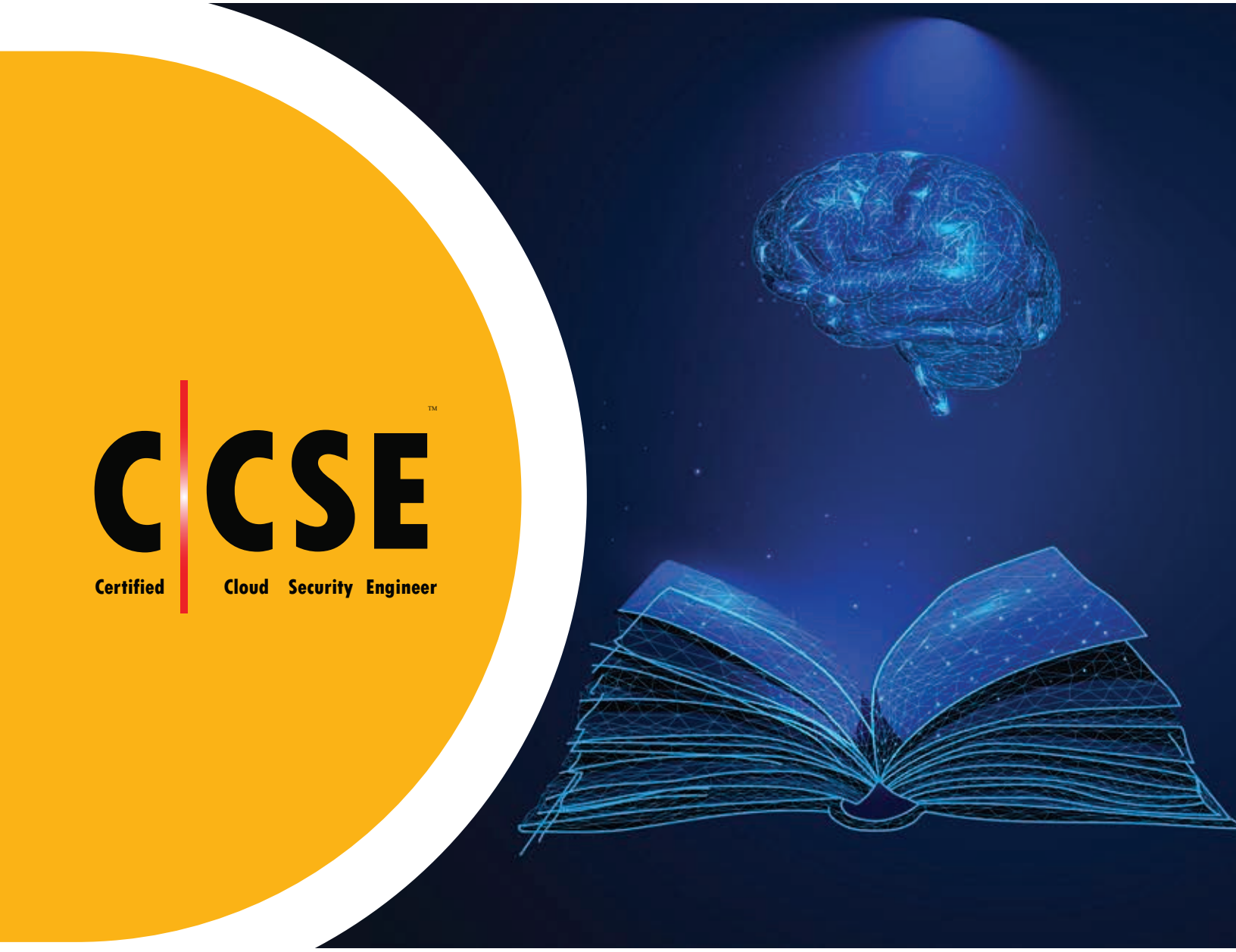
EC-Council



C|CSE™

Certified Cloud Security Engineer

Certified Cloud Security Engineer v1

Course Outline

EC-COUNCIL OFFICIAL CURRICULUM

Certified Cloud Security Engineer (CCSE)v1 Outline

Module 01 Introduction to Cloud Security

LO#01: Understand Cloud Computing Fundamentals

- Cloud Computing
- Cloud Computing Benefits
- Types of Cloud Service Models
- Customer vs CSP Shared Responsibilities in IaaS, PaaS, and SaaS
- Cloud Deployment Models
- NIST Cloud Deployment Reference Architecture

LO#02: Understand Cloud Security Objectives and Issues

- Core Cloud Security Objectives
- Cloud Security Concerns
- Cloud Security Issues
- Core Cloud Security Risks, Threats, Vulnerabilities

LO#03: Understanding Cloud Security Insights

- Cloud Security Vs Traditional Security
- Cloud Security: Shared Responsibility
- Elements of Cloud Security: Consumers Vs Providers
- Identity and Access Management (IAM)
- Data Storage Security
- Network Security
- Monitoring
- Logging
- Compliance

LO#04: Evaluate CSPs for Security before Consuming a Cloud Service

- Evaluating the CSPs
- Security Features Provided By AWS, Azure, and GCP
- On-premise vs Third Party Security Controls Provided by Major CSPs

LO#05: Discuss Security Shared Responsibility Model in Amazon Cloud (AWS)

- Understanding AWS Shared Responsibility Model
- Shared Responsibility Model: Infrastructure Services

- Shared Responsibility Model: Container Services
- Shared Responsibility Model: Abstract Services
- AWS Secured Solution Design

LO#06: Discuss Security Shared Responsibility Model in Microsoft Azure Cloud

- Understand Azure's Shared Responsibility Model
- Azure Secured Solution Design

LO#07: Discuss Security Shared Responsibility Model in Google Cloud Platform (GCP)

- Understanding Google Cloud Shared Responsibility Model
- GCP Secured Solution Design

Module 02: Platform and Infrastructure Security in Cloud

LO#01: Understand Cloud Platform and Infrastructure

- What is Cloud Infrastructure?
  - Cloud Platform and Infrastructure Components
  - Network Component
  - Network Virtualization
  - Microsegmentation and Software-Defined Perimeter (SDP)
  - Cloud Compute Virtualization
  - Storage Virtualization
  - Management Component

LO#02: Understand the Risks and Threats Associated with Cloud Platform and Infrastructure

- Risks Associated with Cloud Platform and Infrastructure
  - Policy and Organization Risks
  - General Risks
  - Virtualization Risks
  - Non-Cloud-Specific Risks
  - Cloud-Specific Risks
  - Legal Risks
- Threats to Cloud Platform and Infrastructure
- Challenges of Virtual Appliances

LO#03: Learn how to Secure the Key Components of Cloud Platform and Infrastructure

- Cloud Platform and Infrastructure Security
- Security of Physical and Environment Component
- Security of Management Component

- Management Component Security Providers Responsibility
- Security of Network Component
- Shared Responsibility Network Virtualization Security
- SDN Security Benefits
- Network Component Security Considerations
- Compute Component Security
- Container Security
- Virtual Machine Image Security
- Storage Component Security
- Virtualization Component Security
- Compute Virtualization Security Shared Responsibility
- Cloud Service Providers Virtualization Security Practices
- Impact of Cloud on Entitlements, Authorization, and Access Management
- Managing Users and Identities for Cloud Computing
- Authentication and Credentials
- IAM Standards for Cloud Computing
- Entitlement and Access Management
- Privileged User Management
- Workload Security
- Standard Workload Security Controls
- Workload Security Monitoring and Logging
- Immutable Workloads to Enhance Security
- Vulnerability Assessment in Cloud Environment
- Risk Audit Mechanisms

LO#04: Learn how to Design a Secure Data Center in Cloud

- Cloud Data Center
- Architecture of Cloud Data Center
- Physical Design Considerations for Data Center
- Physical Network and Storage Design Considerations for Data Centers
- Logical Design Considerations for Cloud Data Center
- Environmental Design of Cloud Data Center

LO#05: Understand Cloud Platform and Infrastructure Security in AWS

- Physical and Environment Security

- Network Service Security: Elastic Load Balancing Security
- Network Service Security: Amazon Virtual Private Cloud (Amazon VPC) Security
- Network Service Security: EC2-VPC Network Access Control Features
- Amazon Route 53 Security
- Amazon CloudFront Security
- Amazon Direct Connect Security
- Compute Service Security: Amazon Elastic Compute Cloud (Amazon EC2) Security
- Compute Service Security: Auto Scaling Security
- Deployment and Management: AWS Identity and Access Management (IAM)

LO#06: Learn how to Implement Cloud Platform and Infrastructure Security in AWS

- Create Security Group to Secure EC2 Instance
- Utilize Separate VPCs to Isolate Infrastructure
- Use AWS Network ACLs to Secure the VPC
- Enable VPC Flow Logs to Monitor Network Traffic
- Secure VPC by Deploying AWS Network Firewall
- Disable Password-Based Remote Logins on Amazon Linux Instance
- Create Amazon EBS Snapshots for Data Backup
- Amazon Infrastructure Security Best Practices

LO#07: Understand Cloud Platform and Infrastructure Security in GCP

- Secure Low-Level Infrastructure
- Secure Service Deployment
- Secure Internet Communication
- Securing the Google Cloud Platform

LO#08: Learn how to Implement Cloud Platform and Infrastructure Security in Google

- Set up the Google Cloud Organization Structure
- Control Access to Google Cloud Resources
- Use Dynamic Routing when possible
- Utilize VPC to Define the Network
- Use Custom-Mode VPC Network in Google Cloud
- Use Shared VPC for Administrating Multiple Working Groups
- Use VPC Flow Logs to Monitor Network Traffic of VMs
- Enforce Compute Engine Rightsizing Recommendations
- Create Firewall Rules to Manage Traffic in GCP

- Infrastructure Security Best Practices

LO#09: Understand Cloud Platform and Infrastructure Security in Microsoft Azure

- Azure Facilities, Premises, and Physical Security
- Azure Infrastructure Availability
- Azure Information System Components
- Azure Network Architecture
- The Azure Production Network Security
- Azure Infrastructure Monitoring
- Azure Infrastructure Integrity

LO#10: Learn to Implement Cloud Platform and Infrastructure Security in Microsoft Azure

- Set up Availability Zones within Azure Region
- Grant Conditional Access to Azure Resources
- Enforce Azure Disk Encryption
- Implement Virtual Network Service Endpoints
- Use Just-in-Time (JIT) to Secure Management Ports
- Implement Hub-Spoke Network Topology
- Disable RDP/SSH Direct Access to VMs in Azure
- Configure Azure Bastion to Secure RDP/SSH Access to Azure VMs
- Use Network Security Group (NSG) to Filter Virtual Network Traffic
- Deploy Azure Firewall to Secure Azure Virtual Network Resources
- Use Azure Security Center
- Infrastructure Security Best Practices

Exercise 01: Implementing AWS Identity and Access Management

Exercise 02: Implementing AWS Key Management Services

Exercise 03: Creating Secure EC2 Instances in AWS Virtual Private Cloud (VPC)

Exercise 04: Implementing Role-Based Access Control in Microsoft Azure

Exercise 05: Deploying a Secure Windows Server VM in Azure with Antimalware Extension Enabled

Exercise 06: Blocking Management Ports with Azure Security Center to Prevent Brute Force Login Attacks on Virtual Machines in Azure

Exercise 07: Implementing Role Based Access Control with GCP IAM

Exercise 08: Securing GCP Instances using Firewall Rules

Exercise 09: Implementing Secure Deployments in GKE with Binary Authorization

Exercise 10: Implementing a Private Secure Connection Between Instances with VPC Network Peering

Module 03 Application Security in Cloud

LO#01: Understand Cloud Application Security

- What is Cloud Application?
- Security Benefits of Cloud Applications
- What is Cloud Application Security?
- Security Challenges of Cloud Applications
- Cloud Application Security Responsibilities across Cloud Service Models

LO#02: Discuss cloud application security risks

- Common Cloud Application Vulnerabilities and Risks – OWASP Top 10
- Focus on Cloud-Specific Risks
- Scope of Cloud Application Security

LO#03: Understand Secure Software Development Lifecycle (SSDLC) of Cloud Applications

- Secure Design and Development
- SSDLC Phases
- Cloud Application Architecture
- Built-in and Add-on Security in Cloud
- Considerations for Designing Secure Application in Cloud
- Best Practices for Secure Cloud application Design and Architectures
- PaaS Security Configuration

LO#04: Understand DevOps and Continuous Integration/ Continuous Deployment (CI/CD)

- Common Cloud Application Deployment Pitfalls
- SSDLC and automated DevOps processes
- Integrate Vulnerability Assesment in CD/CI Pipeline
- Deployment Pipeline Security
- Devops and DevSecOps
- Using Infrastructure as Code for Secure Deployment
- Security activities for Cloud Application Security

LO#05: Discuss cloud application security controls

- Perform Application Threat Modeling
- Ensure Application Data Security
- Design Appropriate Identity and Access Management (IAM) Solutions
- Design Appropriate Identity and Access Management (IAM) Solutions
- Adopt Penetration Testing for Cloud Applications

- Secure Code Reviews
- Implement Quality of Service
- Application Security Testing
- Implement Additional Security Devices for Application Security
- Application Security: Implement Web Application Firewall (WAF)
- Application Security: Database Activity Monitoring (DAM)
- Application Security: Implement Extensible Markup Language (XML) firewalls
- Application Security: Implement Cryptography
- Application Security: Sandboxing
- Application Security: Application Virtualization and orchestration
- Enforce Compliance, Governance, and Security Policies using CASB
- Enforce Compliance, Governance, and Security Policies using CASP
- Implement Runtime Application Self Protection (RASP)
- Cloud Application Security Audit Checklist
- Cloud Application Security Considerations for Cloud Provider
- Cloud Application Security Recommendations

LO#06: Understand Application Security Features in AWS

- AWS Application Security Features
- AWS Identity and Access Management
- AWS WAF – Web Application Firewall
- Amazon Cloud Front
- AWS Shield
- Amazon Inspector
- Amazon Cloud Watch
- Securing Amazon Machine Images (AMI)
- AWS Application Infrastructure Security: Network Security
- AWS Application Security Best Practices

LO#07: Learn How to Implement Application Security in AWS

- AWS IAM: Lock Your AWS Account Root User Access Keys
- AWS IAM: Create Individual IAM Users
- AWS IAM: Use Groups to Assign Permissions to IAM Users
- AWS IAM: Grant Least Privilege
- AWS IAM: Use AWS-managed Policies

- AWS IAM: Use Customer-managed Policies Instead of Inline Policies
- AWS IAM: Use Access Levels to Review IAM Permissions
- AWS IAM: Configure a Strong Password Policy for Users
- AWS IAM: Enable MFA for Privileged Users
- AWS IAM: Use Roles for Amazon EC2 Instances
- AWS IAM: Rotate Security Credentials Regularly
- AWS IAM: Use Roles to Delegate Permissions and Do Not Share Access Keys
- AWS IAM: Remove Unnecessary Credentials
- AWS IAM: Monitor Activity of AWS Account
- AWS IAM Application Security Best Practices
- Application Infrastructure Security: SSL Termination at Application Load Balancer
- Application Infrastructure Security: SSL Termination at Elastic Load Balancer
- Application Infrastructure Security: SSL Termination at Network Load Balancer
- Application Infrastructure Security using Bastion Host
- Securing Application Infrastructure using Systems Manager
- Application Data Security using AWS Secrets Manager
- Detect and Respond to Application Attacks using AWS Config
- Detect and Respond to Application Attacks using VPC Flow Logs
- Detect and Respond to Application Attacks using Amazon Guard Duty

LO#08: Understand Application Security Features in Azure

- Azure Application Security Features
- Azure CDN
- Azure Web Application Firewall
- Azure DDOS Protection Service
- Azure Security Centre
- Azure Monitor
- Azure Application Security Best Practices

LO#09: Learn How to Implement Application Security in Azure

- Azure Threat modeling
- Azure IAM App Security Configuration: Enable Single-Sign-on
- Azure IAM App Security Configuration: Turn on Conditional Access
- Azure IAM App Security Configuration: Implement Role-based Access Control

- Azure IAM App Security Configuration: Implement Password Hash Synchronization with Azure AD Connect Sync
- Securing Application Infrastructure using Azure Front Door
- Securing Application Infrastructure using Traffic Manager
- Securing Application Infrastructure Using Application Gateway
- Securing Application Infrastructure using Azure Load Balancer
- Azure Detection and Response to Threats
- Detect and Respond to Threats using Azure Sentinel
- Detect and Respond to Threats using Microsoft Anti-malware
- Detect and Respond to Threats using Cloud App Security
- Detection and Respond to Threats using Application Insights
- Detect and Respond to Threats using Anomaly Detector

LO#10: Understand Application Security Features in GCP

- GCP Application Security Features
- Web Application and API Protection (WAAP)
- App Engine Firewall
- Cloud Security Scanner
- Cloud Identity Aware Proxy
- Cloud Endpoints
- Secrets Manager

LO#11: Learn How to Implement Application Security in GCP

- GCP IAM Security Configurations for Application Security
- GCP IAM: Rotate Service Account Keys
- GCP IAM: Grant Least Privileges to Avoid Primitive Roles
- GCP IAM: Grant Predefined Roles
- GCP IAM: Create Separate Service Account
- Securing Application Infrastructure
- Detect and Respond to Threats using GCP Operations Suite
- Application Security Tools
- GCP Application Security Best Practices

Exercise 01: Implementing Web Application Firewall in AWS

Exercise 02: Enforcing Principle of Least Privilege with SAML-based Single Sign-on in Azure

Exercise 03: Using Azure AD Multi-Factor Authentication Settings to Block and Unblock Microsoft Azure User

Exercise 04: Restricting Access to App Engine Applications in GCP with Cloud IAP

Module 04 Data Security in Cloud

LO#01: Understand Data Security in Cloud

- What is Cloud Storage?
- Benefits of Cloud Storage
- What is Cloud Data Security?
- Importance of Cloud Data Security

LO#02: Discuss cloud data storage fundamentals

- Cloud Storage Concepts
- Types of Cloud Data Storage
- RAID Technology in Cloud Data Storage
- Storage Techniques in Cloud
- Intelligent Storage Device Components in Cloud
- Cloud Storage Mechanisms
- Cloud Storage Design Patterns

LO#03: Understand the cloud storage architecture and life cycle phases

- Cloud Data Storage Architecture: Volume Storage
- Cloud Storage Architecture: Object-Based Storage
- Cloud Storage Architecture: Cloud Database
- Cloud Storage Architecture: Raw Storage, Long-term Storage, Ephemeral Storage
- Content Delivery Network (CDN)
- Cloud Data Life Cycle Phases

LO#04: Evaluate the risks, attacks, and issues in cloud data storage

- Issue and Threats to Cloud Data Storage
- Best Practices for Cloud Data Storage

LO#05: Understand data security strategies and technologies in the cloud

- Cloud Storage Data Encryption
- Key Management and Encryption Architectures
- Encryption in IaaS, PaaS, and SaaS
- Cloud Storage Encryption Tools: Boxcryptor
- Cloud Storage Encryption Tools: VeraCrypt
- Cloud Storage Encryption Additional Tools
- Enhancing Encryption Strength: Hardware / Software Protection

- Tips to Protect Encryption Keys
- Cloud Data Access Control
- Hashing
- Data Masking
- Tokenization
- Anonymization
- Data Loss Prevention (DLP)
- Data De-Identification and Data Re-Identification
- Data Migration in Cloud
- Manage Data Migration to the Cloud
- Sensitive Data
- Data Protection (Rest, At Transit, In Use)
- Data Redundancy in Cloud
- Geofencing
- Securing Data Transfer in Cloud
- Cloud Data Audit
- Database Activity Monitoring and File Activity Monitoring

LO# 06: Discuss Information Rights management Systems

- Information Rights Management (IRM)
- Challenges with Information Rights Management (IRM)
- Solutions for Successful IRM Implementation

LO# 07: Discuss Data retention and archiving strategies

- Data Retention Policies
- Data Deletion Procedures and Mechanisms
- Data Archiving Procedures and Mechanisms

LO#08: Discuss Storage and Analysis of Data events

- Definition of Event Sources and Requirement of Identity Attribution
- Storage and Analysis of Data Events
- Chain of Custody and Non-repudiation

LO#09: Understand storage services in Amazon Webservices (AWS)

- What is AWS Storage?
- AWS Storage Services: Amazon Simple Storage Service (Amazon S3)
- AWS Storage Services: Amazon Glacier

- AWS Storage Services: Amazon Elastic Block Store (Amazon EBS) Volume
- AWS Storage Services: AWS Storage Gateway
- AWS Storage Services: Amazon Elastic File System (EFS)
- AWS Storage Services: Amazon EC2 Instance Storage
- AWS Storage Services: AWS Snowball
- AWS Storage Services: Amazon CloudFront

LO#10: Learn how to implement data security in Amazon Webservices (AWS)

- Enable Amazon S3 Default
- Enable Server Access Logging for Amazon S3 Bucket
- Block Public Access to S3 Bucket
- Restrict Public Access to S3 buckets via Bucket Policy
- Ensure that Amazon S3 buckets are encrypted with customer-provided AWS KMS CMKs
- Restrict Non-SSL S3 Access to all the Objects in Amazon S3 bucket
- Ensure AWS S3 Buckets Enforce Server-Side Encryption (SSE)
- Grant Private Access to EBS Volume Snapshot
- Create Encrypted EBS Volume
- Delete Unused EBS Volume
- Ensure to Launch an EC2 Instance with Encrypted Volume
- Configure CloudFront Distribution to Compress Objects Automatically
- Enable Geo-Restriction for Amazon CloudFront Distribution
- Configure Viewer Protocol Policy of CloudFront Distribution
- Enable AWS RDS Encryption
- Enable Encryption for AWS Athena Query Results
- Creating Amazon S3 Access Point with VPC
- AWS Snowball Best Practices
- Use KMS CMKs for AWS Storage Gateway File Shares
- Use KMS CMKs for AWS Storage Gateway Tapes
- Use KMS Customer Master Keys for AWS Storage Gateway Volumes
- Ensure that Amazon Backup Service is Used to Manage AWS RDS Database Snapshots
- Enable Lifecycle Configuration for Amazon Backup Plan
- Prevent Deletion of Backups Using an Amazon Backup Vault Resource-Based Access Policy

LO#11: Understand storage services in Google Cloud Platform (GCP)

- What is Google Cloud Storage?

- Features of Google Cloud Storage
- Key Terms of Google Cloud Storage
- Interacting Tools in Google Cloud Storage
- Data Security in Google Cloud Storage
- Google Cloud Object Storage
- Google Cloud Block Storage
- Google Cloud Archival Storage
- Google Cloud File Storage
- Google Cloud Data Transfer Services
- Google Cloud Transfer Appliance
- Firebase
- Google Workspace

LO#12: Learn how to implement data security in Google Cloud Platform (GCP)

- Turn on Uniform Bucket-Level Access
- Enforce Domain-Restricted Sharing Policy
- Enable Cloud KMS to Encrypt Cloud Storage Data
- Audit Cloud Storage Data with Cloud Audit Logs
- Secure Google Cloud Data with VPC Service Controls

LO#13: Understand storage services in Microsoft Azure

- What is Azure Storage?
- Features of Azure Storage
- Types of Azure Storage

LO#14: Learn how to implement data security in Microsoft Azure

- Enable Soft Delete Feature of Azure Blob Storage
- Restrict Access Using SAS
- Enable Secure Transfer Required Feature in Azure Storage Account
- Configure Immutable Policies
- Allow Shared Access Signature Tokens Over HTTPS Only
- Check for Overly Permissive Stored Access Policies
- Select Longer Soft Deleted Data Retention Period
- Enable Blob Storage Lifecycle Management
- Enable Trusted Microsoft Services for Storage Account Access
- Limit Storage Account Access by IP Address

- Check for Key Vault Full Administrator Permissions
- Disable Anonymous Access to Blob Containers
- Use BYOK for Storage Account Encryption
- Enable Logging for Azure Storage Queue Service
- Use soft delete for containers
- Lock storage account to prevent accidental account deletion
- Enable In-Transit Encryption for MySQL Servers
- Enable Transparent Data Encryption for Azure SQL Database
- Create Alert for "Delete Azure SQL Database" Events
- Enable In-Transit Encryption for PostgreSQL Database Servers
- Enable "CONNECTION_THROTTLING" Parameter for PostgreSQL Servers
- Enable LOG_CHECKPOINTS Parameter for PostgreSQL Servers
- Enable LOG_CONNECTIONS Parameter for PostgreSQL Servers
- Enable LOG_DURATION Parameter for PostgreSQL Servers
- Enable Active Geo-Replication of Azure SQL Database
- Configure Azure Defender for Storage
- Ensure to Set Encryption Key Expiration
- Restrict Network Access Using Service Endpoints

Exercise 01: Restricting access to S3 Bucket Object Using CloudFront

Exercise 02: Restricting Access to AWS S3 Buckets using ACL and Bucket Policy

Exercise 03: Restricting Non-SSL Access for S3 Objects using Bucket Policies

Exercise 04: Securing Amazon RDS from Accidental Deletion

Exercise 05: Preventing Deletion of Backups Using an Amazon Backup Vault Resource-Based Access Policy

Exercise 06: Preventing Accidental Deletion and Modification of S3 Objects using S3 Object Lock

Exercise 07: Restricting Access to Azure Storage Account Using Shared Access Signature (SAS)

Exercise 08: Disabling Anonymous Access to Blob Container in Azure

Exercise 09: Preventing Accidental Deletion of Resources Using Azure Resource Locking

Exercise 10: Restricting Network Access to Azure Storage Account Using Virtual Network Service Endpoints

Exercise 11: Protecting Secrets in Azure with Key Vault

Exercise 12: Implementing Encryption and Decryption of Data with Google Cloud KMS

Exercise 13: Inspecting Sensitive Information in GCP with Cloud DLP

Module 05 Security Operations in Cloud

LO#01: Discuss cloud security operations

- What are Cloud Operations?
- What is Cloud Operation Security?
- Fundamentals/Strategies to Secure Cloud Operations

LO#02: Understand elements (standards and methods) in cloud data center physical/logical Operations

- Cloud Data Center Physical/Logical Operations
- Physical/Logical Operations: Facilities and Redundancy
- Physical/Logical Operations: Virtualization Operations
- Physical/Logical Operations: Storage Operations
- Physical/Logical Operations: Physical and Logical Isolation

LO#03: Learn Security Operations to Build Cloud Infrastructure

- Security Configuration Requirements for Cloud Infrastructure
- Hardware Security Configurations
- Virtualization Management Tool
- Virtual Management Tools
- Best Practices for Secure Configuration of Virtualization Management Tools
- Virtual-Hardware Security Configurations
- OS Virtualization Toolset Installations

LO#04: Learn How to Perform Security Operations for Cloud Infrastructures

- Security Configuration Requirements for Running Cloud Infrastructure
- Local and Remote Access Control Configurations
- Secure Network Configuration
- Secure Network Configuration: VLANs
- Secure Network Configuration: Transport Layer Security
- Secure Network Configuration: DNS and DNSSEC (Domain Name System Security Extensions)
- Example: Sonicwall's DNS Sinkhole to Block DNS Queries
- Example: IBM Navigator to Deny Zone Transfers
- Secure Network Configuration: Dynamic Host Configuration Protocol
- Secure Network Configuration: IPSec
- Example: miniOrange 2FA for Fortinet Fortigate VPN
- OS Security Configurations
- Baseline Configuration by Windows

- Baseline Configuration by Linux
- Baseline Configuration by VMware
- Ensuring OS Availability
- How to Achieve High Availability in the Cloud
- Example: IBM Cloud Kubernetes Cluster for HA

LO#05: Learn Security Operations to Manage Cloud Infrastructure

- Cloud Infrastructure Management
- Remote Access Security
- Remote Access Security with Remote Desktop Protocol
- Remote Access Security with Secure Shell
- OS Security Compliance
- Managing Updates in Cloud Infrastructure
  - Hotfix
  - Patch
  - Version Update
  - Rollback
- Cloud Patching Methodologies
  - Production Systems
  - Development Systems
  - Quality Assurance
  - Perform Rolling Updates
  - Blue-Green
  - Clustering and Failover
- Patch Management
- Patch Management: Challenges in Cloud Environment
- Applying Security Patches
- Monitoring Performance and Capacity of Cloud Infrastructure
- Monitoring Hardware of Cloud Infrastructure
- Backup and Restore of Host and Guest OS Configuration
- Network Security Controls
- Network Security Controls: Firewalls
- Network Security Controls: Intrusion Detection System (IDS)
- Network Security Controls: Intrusion Prevention System (IPS)

- Network Security Controls: Honeypots
- Network Security Controls: Vulnerability Assessments
- Network Security Controls: Network Security Groups
- Management Plane

LO#06: Discuss Security Configurations Management for Cloud Infrastructure

- Cloud Operations Management Components
- Information Security Management
- Continuity Management
- Change Management
- Continual Service Improvement Management
- Incident Management
- Problem Management
- Release Management
- Deployment Management
- Configuration Management
- Service-Level Management
- Availability Management
- Capacity Management
- Evidence Management

LO#07: Learn to Monitor Security Operations for Cloud Infrastructure

- Manage Cloud Security Operations
- Manage Communication with relevant Parties
- Security Operations Center
- SOC Capabilities
- Need of SOC
- SOC Key Performance Indicators and Metrics
- Best Practices for Running SOC
- Security Information and Event Management
- Security Analytics
- Need of SIEM
- Typical SIEM Capabilities
- Types of SIEM Solutions
- SIEM Solutions: Micro Focus ArcSight Enterprise Security Manager (ESM)

- SIEM Solutions: Splunk Enterprise Security
- SIEM Solutions: IBM Security QRadar
- SIEM Solutions: AlienVault Unified Security Management (USM)
- Additional SIEM Solutions
- Enforce Standards for Operational Controls: Change Management Implementation
- Enforce Standards for Operational Controls: Incident Management Implementation
- Enforce Standards for Operational Controls: Release and Deploy Management Implementation
- Enforce Standards for Operational Controls: Patch Management Implementation
- Monitor Security Controls Example: Configure UpCloud Firewall
- Monitor Security Controls Example: Add IPS Policy in McAfee Network Security Platform
- Monitor Security Controls Example: Use Nessus Assessment for Vulnerability Assessment
- Monitor Security Controls Example: Implement Honeypot - KFSensor
- Monitor Security Controls Example: Implement IDS: Snort
- Monitor Security Controls Example: Web Vulnerability Assessment

LO#08: Understand security operations in Microsoft Azure

- Azure Operational Security
- Azure Monitor
- Azure Security Center
- Network Watcher
- Azure Storage Analytics
- Azure Active Directory
- Azure Automation

LO#09: Learn to implement security operations in Microsoft Azure

- Manage and Monitor User Passwords
- Configure Azure Service Health alerts to get incident notifications
- Manage Subscriptions using Management Groups
- Streamline Environment Creation with Blueprints
- Monitor Storage Services for Unexpected Behavioral Changes
- Prevent, Detect, and Respond to Threats using Azure Sentinel
- View Secure Score using Security Center dashboard
- Discover and Prioritize security issues using Security Center
- Integrate Azure Security Center (ASC) alerts into a SIEM
- Enable Microsoft Defender for Endpoint Detection Integration

- Monitor End-to-End Scenario-Based Network Monitoring
- Secure Deployment using Proven DevOps Tools
- Mitigate and Protect against DDoS
- Monitor Organizations Policies by Enabling Azure Policy
- Monitor Azure AD Reports
- Use Azure Automation to Automate Tasks
- Azure Operational Security Best Practices
- Azure Operations Security Checklist

LO#10: Understand security operations in Amazon Webservices (AWS)

- AWS Security Operations Features/Services
- AWS Systems Manager Explorer
- AWS System Manager OpsCenter
- CloudWatch Dashboards Hosted by Systems Manager
- Trusted Advisor and Personal Health Dashboard (PHD) Hosted by Systems Manager
- AWS CloudTrail
- AWS Config
- Amazon GuardDuty
- Amazon Inspector
- AWS Security Hub

LO#11: Learn to implement security operations in Amazon Webservices (AWS)

- View Events with CloudTrail Event History
- Monitor and Record AWS Resource Configurations using AWS Config
- Use Amazon CloudWatch to Monitor AWS Resources
- Monitor GuardDuty Findings with Amazon CloudWatch Events
- Enable and Analyze VPC Flow Logs in AWS
- Use CloudFormation StackSets for Provisioning Resources

LO#12: Understand security operations in Google Cloud Platform (GCP)

- GCP Operational Security
- Security Analytics and Operations
- Security Command Center (SCC)
- Cloud Monitoring
- Cloud Identity
- Google Cloud's Operation Suite

LO#13: Learn to implement security operations in Google Cloud Platform (GCP)

- Use Google Cloud Security Scanner to Scan Vulnerabilities in Google App Engine Web Apps
- Use VPC Flow Logs to Record Traffic Flow
- Use GCP Firewall Rules Logging to Analyze, Verify and Audit Effects of Firewall Rules
- Use Cloud Monitoring to Investigate Incidents
- Use Google Security Command Center Dashboard to Detect and Prevent Threats

Exercise 01: Discovering Potential Security Issues using Amazon Inspector

Exercise 02: Monitoring User Activity using AWS CloudTrial

Exercise 03: Notifying Security Group Change using CloudTrail and CloudWatch

Exercise 04: Restrict Remote Desktop Access to Virtual Machines Using Network Security Group (NSG) in Azure

Exercise 05: Secure RDP/SSH Access to Azure Virtual Machines Using Azure Bastion

Exercise 06: Scanning for Vulnerabilities in App Engine Applications with Google Cloud Web Security Scanner

Module 06: Penetration Testing in Cloud

LO#01: Understand the scope of cloud penetration testing

- Penetration Testing in Cloud Computing
- Do Remember: Cloud Penetration Testing
- Scope of Cloud Pen Testing

LO#02: Learn generic penetration testing steps in the cloud

- Understand Shared Responsibilities in Cloud
- Understand Penetration Testing Process, Policies, and Limitations
- Identify the Type of Cloud to be Tested
- Identify what is to be Tested in the Cloud Environment
- Identify Tools for Penetration Testing
- Perform Cloud Reconnaissance
- Check for Lock-in Problems
- Check for Governance Issues
- Check for Compliance Issues
- Check for Right Implementation of Security Management
- Check the Cloud for Resource Isolation
- Check whether Anti-Malware Applications are Installed and Updated on Every Device
- Check whether Firewalls are Installed at Every Network Entry Point
- Check that Strong Authentication is Deployed for Every Remote User

- Check the SSL Certificates for the Cloud Services in the URL
- Check whether Files Stored on the Cloud Servers are Encrypted
- Check the Data Retention Policy of Service Providers
- Check that all Users Follow Safe Internet Practices
- Perform a Detailed Vulnerability Assessment
- Try to Gain Passwords to Hijack the Cloud Service
- Test for Virtualization Management (VM) Security
- Check Audit and Evidence-Gathering Features in the Cloud Service
- Recommendations for Cloud Testing

LO#03: Learn AWS-specific penetration testing steps

- Understand AWS Penetration Testing Policy and Procedures
- Attempt to Identify S3 Buckets
- Check for S3 Bucket Permissions
- Attempt to Create New Policy Version
- Attempt to Set an Existing Policy Version as Default
- Attempt to Obtain Access to the set of EC2 Instance/Role Permissions
- Attempt to Create a New User Access Key
- Attempt to Create a New Login Profile
- Attempt to Update an Existing Login Profile
- Attempt to Attach a Policy to a User
- Attempt to Attach a Policy to a Group
- Attempt to Attach a Policy to a Role
- Attempt to Create/Update an Inline Policy for a User
- Attempt to Create/Update an Inline Policy for a Group
- Attempt to Create/Update an Inline Policy for a Role
- Attempt to Add a User to a Group
- Attempt to Update AssumeRolePolicyDocument of a Role

LO#04: Learn Azure-specific penetration testing steps

- Understand Azure Penetration Testing Policy and Procedures
- Assess Azure Environment with Azure Security Center
- Check Assigned Role of Users
- Check whether access to the Azure AD Portal is Restricted
- Check whether Multi-Factor Authentication (MFA) is Enabled for Every User

- Check whether WAF is installed on Microsoft Azure
- Check whether Data is Encrypted at Rest
- Check whether Azure SQL Databases are Encrypted
- Check the Data Retention Time in Microsoft Azure
- Check whether Network Security Groups Diagnostic logs are turned On
- Check whether Azure Network Watcher is Enabled
- Check whether JIT VM Access is Enabled

LO#05: Learn GCP-specific penetration testing steps

- Understand Google Cloud Shared Responsibility Model
- Google Cloud's Provision for Penetration Testing
- Check whether Security Health Analytics is Enabled
- Check whether Cloud Web Security Scanner is Enabled
- Check whether Cloud Anomaly Detection is Enabled
- Check whether Container Threat Detection is Enabled
- Check whether Event Threat Detection is Enabled

Exercise 01: Identifying Misconfigured S3 Buckets in AWS

Exercise 02: Identifying Publicly Accessible Data with compromised AWS API Keys

Module 07: Incident Response in Cloud

LO#01: Understand Cloud Incident Response

- What is Incident Detection in the Cloud?
- What is Cloud Incident Response?
- Importance of Cloud Incident Response (CIR)
- How is Cloud Incident Response (CIR) different from traditional IR?

LO#02: Understand Cloud Incident Response Lifecycle

- Cloud Incident Response Framework
- Cloud Incident Response Lifecycle: Preparation
- Cloud Incident Response Lifecycle: Detection & Analysis
- Cloud Incident Response Lifecycle Containment
- Cloud Incident Response Lifecycle: Eradication
- Cloud Incident Response Lifecycle: Recovery
- Cloud Incident Response Lifecycle: Post-mortem
- Cloud Incident Response Lifecycle: Coordination and Information Sharing
- Incident Handling Recommendations: Preparation

- Incident Handling Recommendations: Detection & Analysis
- Incident Handling Recommendations: Containment, Eradication & Recovery
- Incident Handling Recommendations: Post-incident Activity
- Managing SaaS Applications' Cybersecurity Incidents
- Cloud Incident Response Best Practices

LO#03: Understand How SOAR Accelerates Incident Response

- Security Orchestration, Automation, and Response (SOAR)
- SOAR Use Cases
- Implementing SOAR in the Cloud: Factors to be Considered
- SOAR Tool: IBM Security SOAR
- SOAR Tool: InsightConnect
- Additional SOAR Tools
- Implementing SOAR Solution: Provisioning and Deprovisioning Users
- Implementing SOAR Solution: Phishing Attack
- Implementing SOAR Solution: Malware Containment
- Implementing SOAR Solution: Alert Enrichment
- Implementing SOAR Solution: Threat Hunting
- Implementing SOAR Solution: Patching and Remediation
- Implementing SOAR Solution: Reduce Alarm Fatigue with Use Case Automation
- Implementing SOAR Solution: Streamline the Security Operations Workflow

LO#04: Discuss Security Incident Response in AWS

- AWS Cloud Adoption Framework
- AWS Incident Response Plan
- Design Goals of Responding to Cloud Incidents
- Indicators of Cloud Security Events
- AWS Incident Response Domains
- Incidents in Infrastructure Domain
- Incidents in Service Domain
- Incidents in Application Domain
- AWS Incident detection and Response Capabilities
- AWS Incident Response Plan: Educate
- AWS Incident Response Plan : Prepare
- AWS Security Incident Response Plan: Simulation

- AWS Incident Response Plan: Iterate
- AWS Incident Response Plan: Automate

LO#05: Discuss AWS Investigation and Detection Tools

- AWS Investigation and Detection Tools
- AWS Investigation and Detection: Third-Party Tools

LO#06: Discuss Security Incident Response in Microsoft Azure Cloud

- Azure Incident Response Lifecycle
- Preparation
- Set up Azure Security Center Security Contact
- Detection and Analysis
- Use ASC Data Connector to Stream Alerts to Azure Sentinel
- Export ASC Alerts and Recommendations using the Export Feature to Identify Risks
- Capture Network Flow Logs using Azure Network Watcher
- Capture Network Flow Logs using Azure Monitor
- Use Azure VM's Snapshot Feature to Create a Snapshot of the Running System Disk
- Azure IR Features: Azure Security Center
- Azure IR Features: Azure Sentinel
- Investigate Incidents with Azure Sentinel
- Use Tags to Categorize Resources
- Containment, Recovery, and Eradication
- Configure Workflow Automation in Azure Security Center
- Set up Automated Threat Responses in Azure Security Center
- Set up Automated Threat Responses in Azure Sentinel
- Azure IR Best Practices

LO#07: Discuss Security Incident Response in Google Cloud Platform (GCP)

- Google Security Incident Detection and Response
- Google Data Incident Response Process
- Google Data Incident Response Team
- Google Incident Monitoring: Cloud Operations Suite
- Incident Detection and Response: Security Command Centre
- Security Command Centre: Container Threat Detection
- Security Command Centre: Event Threat Detection
- Security Command Centre: Cloud Anomaly Detection

- Security Command Centre: Security Health Analytics
- Security Command Centre: Web Security Scanner
- Packet Mirroring
- Automated Application Incident Response by Cloud Armor
- VPC Service Controls
- Google Cloud Status Dashboard
- Prevent, Detect and Respond to Threats with Security Command Centre Dashboard
- Responding to Misconfigurations with Security Health Analytics
- Detecting Web Application Vulnerabilities with Cloud Web Security Scanner
- Setting Up Container Threat Detection in Security Command Centre
- Detecting and Responding to threats with Event Threat Detection
- Detecting and Responding to Security Anomalies with Cloud Anomaly Detection
- Stopping Data Exfiltration using Cloud DLP
- Setting Up Packet Mirroring for Monitoring Vulnerabilities
- VPC Flow Logging for Monitoring Network Packets
- Firewall Rules for Monitoring Network Traffic
- Detecting and Responding to Incidents via Cloud Monitoring

Exercise 01: Detecting Compromise of Sensitive Data in S3 Buckets with Amazon Macie

Exercise 02: Creating Activity Log Alerts with Azure Monitor

Exercise 03: Monitoring Network Traffic with VPC Flow Logs in GCP

Exercise 04: Detecting Incidents in GCP with Cloud Monitoring

Module 08 Forensic Investigation in Cloud

LO#01: Discuss cloud forensics

- Usage of Cloud Forensics
- Cloud Crimes
- Cloud Forensics: Stakeholders and their Roles
- Cloud Forensics Challenges: Architecture and Identification
- Cloud Forensics Challenges: Data Collection
- Cloud Forensics Challenges: Logs
- Cloud Forensics Challenges: Legal
- Cloud Forensics Challenges: Analysis

LO#02: Learn how to investigate security incidents in Amazon Web Services (AWS)

- Forensic Acquisition of Amazon EC2 Instance: Methodology

- Step 1: Isolate the Compromised EC2 Instance
- Step 2: Take a Snapshot of the EC2 Instance
- Step 3: Provision and Launch a Forensic Workstation
- Step 4: Create Evidence Volume from the Snapshot
- Step 5: Attach the Evidence Volume to the Forensic Workstation
- Step 6: Mount the Evidence Volume on the Forensic Workstation
- Investigating Log Files: CloudWatch Logs
- Investigating Log Files: S3 Server Access Logs

LO#03: Learn how to investigate security incidents in Microsoft Azure

- Forensic Acquisition of VMs in Azure: Methodology
- Forensic Acquisition of VMs in Azure: The Scenario
- Step 1: Create a Snapshot of the OS Disk of the Affected VM via Azure Portal
- Step 1: Create a Snapshot of the OS Disk of the Affected VM via Azure CLI
- Step 2: Copy the Snapshot to a Storage Account under a Different Resource Group
- Step 3: Delete the Snapshot from the Source Resource Group and Create a Backup Copy
- Step 4: Mount the Snapshot onto the Forensic Workstation
- Analyze the Snapshot via Autopsy
- Data Storage in Azure
- Logs in Azure

LO#04: Learn how to investigate security incidents in Google Cloud Platform (GCP)

- Google Cloud Platform (GCP) Forensics
- Investigating a Security Incident in GCP: Methodology
- Step 1: Collect All the Logs
- Step 2: Take a Snapshot of the Disk of Host VM
- Step 3: Restrict Access to the Host VM
- Step 4: Examine the Snapshot using Docker-Explorer
- Step 5: Redeploy the Container
- Step 6: Delete the Workload

Exercise 01: Examining Logs on Amazon CloudWatch Console

Exercise 02: Forensically Acquiring and Examining VM in Microsoft Azure

Module 09: Business Continuity and Disaster Recovery in Cloud

LO#01: Discuss Cloud Disaster Recovery and Business Continuity

- Cloud Disaster Recovery (CDR)

- Disaster Recovery Objectives
- Cloud vs. Traditional Disaster Recovery
- Disaster Recovery Plan (DRP) in Cloud
- Business Continuity in Cloud
- Business Impact Analysis and Risk Assessment
- Backup and Disaster Recovery in Cloud
- Cloud Disaster Recovery Options
- Disaster Recovery Sites
- Fail over & Fail Back
- Role of Cloud Infrastructure in BC/DR
- Role of Software-Defined Infrastructure in BC/DR
- Role of Infostructure in BC/DR
- Role of Applistructure in BC/DR

LO#02: Learn to Design Disaster Recovery and Business Continuity in Cloud

- Designing a Disaster Recovery Plan in Cloud
- Designing a Business Continuity Plan in Cloud
- Do’s and Don'ts in Cloud Disaster Recovery Planning
- Cloud BC/DR Architecture for Services Already Hosted in the Cloud
- Cloud BC/DR Architecture for In-House/Traditional Non-Cloud Services
- Cloud BC/DR Architecture for PaaS
- Cloud BC/DR Architecture for IaaS and SaaS
- Disaster Recovery as a Service (DRaaS)
- Cloud BC/DR Recovery as a Service (RaaS)
- Business Continuity During Cloud Service Provider Outage
- Business Continuity Within the Cloud Provider
- Business Continuity for Private Cloud and Private Cloud Providers
- BCDR Implementation Guidelines
- Disaster Recovery Checklist
- Disaster Recovery (DR) Test
- Disaster Recovery (DR) Test: Factors & Checklist

LO#03: Learn to Architect Recovery and Resilience in AWS

- AWS DR Topology Map
- Ascending Levels of DR Options

- Backup and Restore Architecture
- Pilot Light Pattern
- Warm Standby Architecture
- Hot Multi-Site Architecture
- AWS DR Features
- AWS Disaster Recovery Features and Services: Deployment Orchestration
- AWS Disaster Recovery Features and Services: Database
- AWS Disaster Recovery Features and Services: Storage
- AWS Disaster Recovery Features and Services: Compute
- AWS Disaster Recovery Features and Services: Networking
- Detection of Disaster Event in AWS
- Testing Disaster Recovery in AWS

LO#04: Learn to Implement Recovery and Resilience in AWS

- Enable Point-in-Time Recovery in AWS DynamoDB Tables
- Create Full Backups of Tables in AWS DynamoDB
- Restore Full Backups of Tables in AWS DynamoDB
- Enable Automatic Backup for RDS DB Instance
- Create EBS Volume Backup as Snapshot
- Check EBS Volumes Snapshots
- Store the Copy of EBS Volume Snapshot in a Different Region
- Restore Volume from EBS Snapshot
- Enable Fast Snapshot Restore
- Business Continuity Plan (BCP): Business Impact Analysis (BIA) and Risk Assessment
- Tips for Developing a Robust Disaster Recovery Plan
- Best Practices for AWS Disaster Recovery Planning
- AWS Partner Network (APN) Partners
- AWS Partner: Sungard Availability Services
- AWS Partner: Commvault
- AWS BCDR Tool: CloudEndure Disaster Recovery
- AWS BCDR Tool: Zerto
- Additional AWS BCDR Tools

LO#05: Understand Business Continuity and Disaster Recovery in Microsoft Azure

- Need for Microsoft Azure Disaster Recovery Service

- Azure Strategies for Business Continuity and Disaster Recovery
- Azure Backup Architecture
- Recovery Services Vault
- Security of Azure Backup
- Azure File Sync
- Linux Application Consistent Backup
- Azure Backup: Restore-as-a-Service
- Enhanced Security for Backups
- Isolation and Access Control
- Azure Backup Monitoring
- Azure Site Recovery
- Features of Site Recovery
- How to Use Azure Site Recovery (ASR)
- Safeguarding VMs Utilizing ASR
- Enterprise Benefits of Azure Disaster Recovery Services
- BCDR in Azure Paired Regions
- Azure Regional Outage Preparation

LO#06: Learn Disaster Recovery Configurations in Azure

- Disaster Recovery Configuration in Azure
- Active-Active-Active (always-on) Configuration
- Active-Active configuration
- Active-Hot standby configuration
- On-demand data recovery configuration

LO#07: Learn to Implement BC/DR with Azure SQL Database

- SQL Database BCDR Features
- Capabilities of Azure SQL Database to Recover from an Outage
- Database restoration within the same Azure region
- Recover a database to the existing server

LO#08: Learn to Configure BCDR for Azure Stack Edge VPN

- BCDR for Azure Stack Edge VPN: Configure failover to a paired region
- BCDR for Azure Stack Edge VPN: Recover from a failed Azure region

LO#09: Understand Various Disaster Recovery Scenarios in Azure

- DR Scenario: Physical Server to Azure

- DR Scenario: VMware to Azure
- DR Scenario: Hyper-V to Azure
- DR Scenario: Azure to Azure
- DR Scenario: VMware/Physical Server to Azure
- DR Scenario: Hyper-V Replication to a Secondary Site
- Enterprise-Scale Business Continuity and Disaster Recovery
- Best Practices for Enterprise Scale Business Continuity and Disaster Recovery (BCDR)
- Backup and Disaster Recovery for Azure Applications

LO#10: Learn to Implement BCDR in Azure

- Enable Automated Backups
- Enable Geo-Redundant Backups
- Enable Email Notifications for Backup Alerts
- Verify Point in Time Restore (PITR) Backup Retention Period
- Configure and Enable Azure Backup Service for VM
- Configure Azure SQL Database to Utilize Auto-Failover Groups
- Configure Automatic Failover for Azure Cosmos DB

LO#11: Discuss Azure Partner Solutions for BCDR

- Veeam
- Commvault
- Additional Partners Solutions for Implementing BCDR in Azure
- Best Practices of Azure Backup and Disaster Recovery

LO#12: Discuss BC/DR in Google Cloud Platform (GCP)

- GCP Features for Business Continuity and Disaster Recovery
- GCP Tools/Services for DR Plan

LO#13: Discuss GCP Resources for Disaster Recovery (DR) and Business Continuity Plan (BCP)

- GCP Services Utilized in BCDR
- Google Cloud Compute Features for BCDR
- Google Cloud Networking and Data Transfer Features for BCDR
- Google Cloud Management and Monitoring Features for BCDR
- Google Cloud Cross-Platform Tools for BCDR
- Things to Consider While Planning a DR Architecture

LO#14: Understand Disaster Recovery for Data in GCP

- Disaster Recovery for Data in GCP

- On-Premises Production Environment: Data Backup and Recovery
- On-Premises Production Environment: Database Backup and Recovery
- Google Cloud Production Environment: Data Backup and Recovery
- Google Cloud Production Environment: Database Backup and Recovery
- When the Production Environment is Another Cloud

LO#15: Understand Disaster Recovery for Applications in GCP

- Disaster Recovery for Applications
- Disaster Recovery and High-Availability Architectures for On-Premises Applications
- Disaster Recovery and High-Availability Architectures for Applications on Google Cloud

LO#16: Learn to Architect DR for Cloud Infrastructure Outages

- Architect DR for Cloud Infrastructure Outages

LO#17: Learn to Implement BCDR in Google Cloud Platform (GCP)

- Enable Point-in-Time Recovery
- Create Read Replicas in GCP
- Initiate Failover in GCP
- Enable Replication in Cloud SQL Instances
- Restoring an Instance from Backup
- Checking the Replication Status using Custom Dashboard
- Perform Regional Migration of the Database

LO#18: Discuss Partners Solutions for Implementing BCDR in GCP

- Veeam for GCP BCDR
- Actifio for GCP BCDR
- Zerto for GCP BCDR
- Additional Partners Solutions for Implementing BCDR in GCP

Exercise 01: Implementing Backup of Amazon S3 Objects with Cross Region Replication

Exercise 02: Recovering EC2 Instance using AMI backup option

Exercise 03: Implementing Disaster Recovery in Azure using Storage Data Replication and Failover

Exercise 04: Implementing Backup and Restore of Virtual Machines with Azure Backup

Exercise 05: Creating Snapshot of a VM instance and Restoring the instance using the Snapshot in GCP

Exercise 06: Ensuring Service Availability with HTTP Load Balancing in GCP

Module 10: Governance, Risk management, and Compliance in Cloud

LO#01: Understand GRC in the Cloud

- What is GRC in the cloud?

- Why Does an Organization Need GRC?
- Benefits of GRC in the Cloud
- GRC Use Cases
- GRC Tools
- GRC Tool: StandardFusion
- GRC Tool: IBM OpenPages with Watson
- Additional GRC Tools
- Recommendations for Effective GRC in the Cloud

LO#02: Discuss Cloud Governance

- What is Cloud Governance?
- Need for Cloud Governance
- Importance of Cloud Governance
- Elements of Cloud Governance
- Cloud Computing Governance Principles
- Key Objectives for Cloud Security Governance
- Landscape of Governance Models and Standards
- Key Benefits of a Cloud Governance Framework
- Cloud Computing Challenges for Governance
- Cloud Security Governance Challenges and Solutions
- Cloud Computing Governance Processes
- Cloud Computing Governance Process Pairs
- Cloud Computing Governance Roles
- Cloud Computing Governance Metrics
- Role of IT Governance in Cloud Computing
- Upgrade and Publish Policies, Processes, and Procedures
- Disciplines of Cloud Governance
- Information/Data Governance
- Effect of Cloud Computing on Information/Data Governance Domain
- Best Practices for Information/Data Governance

LO#03: Learn to Implement and Maintain Governance for Cloud Computing

- How to Design and Implement a Cloud Governance Framework?
- Establishing Cloud Governance
- Applying Cloud Computing Governance

- Implementing Governance as a New Concept
- Extending IT Governance Framework in Cloud with Cloud Governance Dial

LO#04: Discuss Risk management in the Cloud

- Cloud Computing Risks
- What is Cloud Risk Management?
- Need for Risk Management in Cloud Computing
- Choices Involved in Managing Risk
- Principles of Cloud Computing Risk
- Cloud Computing Risk Categories
- Cloud Computing Risk Categories (Contd.)
- Cloud Computing Risk Types
- Enterprise Risk Management in Cloud Computing
- Risk Mitigation
- Risk Management Metrics
- Contracts and Service-level Agreements (SLAs)
- Cloud Contract Design and Management for Outsourcing
- Identifying Appropriate Supply Chain and Vendor Management Processes
- Cloud Computing Certification
- CSA Security, Trust, and Assurance Registry (STAR) Supply Chain Risk

LO#05: Discuss Risk Management Framework and Process in the Cloud

- Risk Management Framework
- Cloud Provider's Risk Management Process
- Cloud Consumer's Risk Management Process

LO#06: Understand Cloud Compliance

- What is Cloud Compliance?
- Steps to Compliance in the Cloud
- How to Maintain Cloud Compliance
- Cloud Compliance Challenges
- Consequences of Failure to Achieve Compliance
- Maintaining Compliance When Working with the Cloud
- Tips for Better Cloud Compliance
- Recommendations for Compliance Audits
- Cloud Compliance Checklist

- Cloud Compliance Frameworks: HIPAA
- Cloud Compliance Frameworks: GLBA
- Cloud Compliance Frameworks: GDPR
- Cloud Compliance Frameworks: ITAR
- Cloud Compliance Frameworks: FISMA
- Cloud Compliance Frameworks: FITARA
- Security Centric Frameworks: ISO 27001
- Security-centric Frameworks: NIST
- Security-centric Frameworks: CIS Controls
- Security-centric Frameworks: CSA STAR
- Cloud Compliance Tool: CloudGuard Dome9
- Cloud Compliance Tool: Lacework

LO#07: Learn to Implement GRC in the cloud

- Considerations for an Effective IT GRC Cloud Program
- Implementation of Cloud GRC
- Best Practices for Effective GRC in the Cloud

LO#08: Understand GRC in Amazon Web Services (AWS)

- AWS Security and Compliance Shared Responsibility Model
- Evaluating and Integrating AWS Controls
- AWS Risk and Compliance Program
- Governance in AWS
- Steps to Implement Governance in AWS
- Governance Tools in AWS
- Governance Tools in AWS: AWS Console Mobile Application
- Governance Tools in AWS: AWS License Manager
- Governance Tools in AWS: AWS Managed Services
- Risk Management in AWS
- Compliance in AWS
- Customer Cloud Compliance Governance
- Automate Compliance with AWS CloudFormation

LO#09: Understand GRC in Azure

- Azure Governance Features and Services
- Azure Management Groups

- Azure Policy
- Azure Blueprints
- Azure Resource Graph
- Azure Cost Management
- Operationalizing Azure Secure Score
- Prioritizing Investments on Security Best Practices
- Managing Connected Tenants
- Clear Lines of Responsibility
- Enterprise Segmentation Strategy
- Security Team Visibility
- Assigning Privileges for Managing the Environment
- Assigning Privileges for Managing the Environment: Core Service Reference Permissions
- Assigning Privileges for Managing the Environment: Segment Reference Permissions
- Monitoring Identity Risk
- Discovering and Remediating Common Risks
- Improving Regulatory Compliance with Azure Security Center

LO#10: Understand GRC in Google Cloud Platform (GCP)

- Inbuilt Features for Governance and Risk Management in GCP
- GCP Governance and Risk Management Feature Cloud Discover: Security
- GCP Governance and Risk Management Feature Policy Intelligence
- GCP Governance and Risk Management Feature Google Cloud Adoption Framework
- GCP Governance and Risk Management Feature: G Suite Security Center
- Certifications, Audits, and Assessments in GCP
- Regulatory Compliances: HIPAA
- Regulatory Compliances: GDPR
- Other Regulatory Compliances
- Google Vault
- Compliance Reports Manager
- Custom Governance

Exercise 01: Restricting Deployment of S3 Buckets to a Specific Region using IAM Policy in AWS

Exercise 02: Investigating Compliance Findings using AWS Security Hub

Exercise 03: Enforcing Compliance by Assigning In-built Policy and Creating Custom Policy in Azure

Module 11: Standards, Policies and Legal Issues in Cloud

LO#01: Understand Laws Impacting Cloud Computing

- Legal Risks in Cloud Computing
- Laws Impacting Cloud Computing
- Legal Challenges in Cloud Computing
- Cloud Computing Legal Checklists/Checklist for Protection of Information
- Cloud Computing Legal Checklists/Checklist for Contract Termination
- Cloud Computing Legal Checklists/Checklist for Liability
- Cloud Computing Legal Checklists/Checklist for Performance management
- Cloud Computing Legal Checklists/Checklist for Handling Legal Issues in Cloud Provider Selection

LO#02: Learn the Cloud Computing Standards

- Need for Standards in Cloud Environments
- What Should be Standardized?
- Benefits of Standardized Policies
- Cloud Security Standards: PCI DSS
- Cloud Security Standards: ITU-T X.1601
- Cloud Security Standards ISO/IEC 27017
- Cloud Security Standards: ISO/IEC 27018
- Cloud Security Standards: NIST
- Cloud Security Standards: CSA Cloud Controls Matrix (CSA CCM)
- Cloud Security Standards: SAML 2.0
- Cloud Security Standards: Open Virtualization Format (OVF)
- Cloud Security Standards: Open Cloud Computing Interface (OCCI)
- Cloud Security Standards: Cloud Data Management Interface (CDMI)
- Role of Cloud Standard Organizations
- Activities of Different Cloud Standard Organizations
- Organizations Involved in Development of Standards for Cloud Computing
- Cloud Standards Organizations: National Institute of Standards and Technology (NIST)
- Cloud Standards Organizations: Cloud Security Alliance (CSA)
- Cloud Standards Organizations: Distributed Management Task Force (DMTF)
- Cloud Standards Organizations: Open Cloud Consortium (OCC)
- Cloud Standards Organizations: Open Grid Forum (OGF)
- Cloud Standards Organizations: The Object Management Group (OMG)

- Cloud Standards Working Committees: Storage Networking Industry Association (SNIA)
- Cloud Standards Organizations: Institute of Electrical and Electronics Engineers (IEEE)
- Cloud Standards Organizations: European Telecommunications Standards Institute (ETSI)
- Cloud Standards Organizations: Organization for the Advancement of Structured Information Standards (OASIS)

LO#03: Describe the Legal Frameworks for Data Protection and Privacy

- Legal Frameworks for Data Protection and Privacy
- Features of Legal Frameworks for Data Protection and Privacy
- Regional Legal Frameworks: Asia-Pacific Region
- Regional Legal Frameworks: European Union And European Economic Area
- Regional Legal Frameworks: The Americas
- Contracts and Provider Selection
- Electronic Discovery
- Recommendations for Handling Legal Issues, Cloud Contracts, and e-Discovery

LO#04: Learn Audit Planning and Reporting in the Cloud

- Cloud Computing Audit
- Potential Impact of Cloud Auditing on the Organization
- Scope, Objectives, and Context of Cloud Auditing for Audit Planning
- Testing Methods in Cloud Auditing
- Sample Audit Tests/Procedures
- Internal Audit
- Objectives of Internal Audits and Internal Auditors
- Cloud-specific Auditing Challenges
- Standards Applicable to Cloud Security Auditing
- Gap Analysis

LO#05: Describe Outsourcing and Vendor Management

- Cloud Computing Contracts
- Questions to Ask Before Signing a Cloud Computing Contract
- Non-Negotiable Contracts
- Issues with Subcontracts
- Business Continuity and Interoperability Issues
- Best Practices for Cloud Computing Contracts
- Contract requirements for Cloud Security

- Examining SLAs
- Vendor Transitioning

LO#06: Understand Standards, Policies, and Auditing in AWS

- AWS Compliance Programs
- AWS Audit Manager
- Audit Preparation with AWS Audit Manager
- AWS Security Auditing Checklist

LO#07: Understand Standards, Policies, and Auditing in Azure

- Azure Compliance Offerings
- Azure Policy
- Create Policy Assignment to Identify Non-Compliant Resources
- Auditing for SQL Database and Synapse Analytics in Microsoft Azure
- Recommendations for Azure Audit Services

LO#08: Understand Standards, Policies, and Auditing in GCP

- Google Cloud Compliance Offerings
- GCP Audit Logs
- Auditing in GCP with Cloud Audit Logs
- Best practices for Cloud Audit Logs

Exercise 01: Conducting Security Audit in AWS with AWS trusted Advisor

Exercise 02: Auditing Compliance of Azure Resources by creating Policy Assignments with Azure Policy

Exercise 03: Conducting Audit in GCP with Cloud Audit Logs