INFOSECTRAIN

# Cloud Security Expert

Course Content

sales@infosectrain.com | www.infosectrain.com

# Course Content

1. Module 1: (Mapped to AWS Certified Security – Specialty)
2. Module 2: (Mapped to Azure AZ-500)
3. Module 3: (Mapped to CCSP)

# Module 1 (Mapped to AWS Certified Security – Specialty)

## Domain 1: Incident Response

- Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys.
- Preparation stages for incident response
- Mitigation steps to perform Incident response steps
- Verify that the Incident Response Plan includes relevant AWS services
- Evaluate suspected compromised credentials
- Evaluate suspected compromised EC2 Instances
- AWS Guard Duty
- Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

## Domain 2: Logging and Monitoring

- Design, Implement & troubleshoot security monitoring and alerting.
- Design, Implement & troubleshoot a logging solution.
- Continuous Security Monitoring
- AWS Security Solutions for Visibility and Compliance
- AWS Inspector
- AWS Detective & Security Hub
- AWS WAF and Shield
- AWS Systems Manager
- AWS CloudWatch, CloudTrail and Config
- AWS Athena
- AWS Macie
- S3 Events & VPC Flow Logs

## Domain 3: Infrastructure Security

- Design edge security on AWS.
- Design and implement a secure network infrastructure.
- Troubleshoot a secure network infrastructure
- Design and implement host-based security
- AWS CloudFront
- Security groups & Network ACLs
- IPS/IDS concepts in cloud
- DDoS Mitigation
- Network Segmentation
- Bastion Hosts
- Virtual Private Cloud (VPC)
- VPC Endpoints
- Compliance Frameworks
- AWS lambda fundamentals
- AWS Simple Email Service
- AWS Route53 DNS

## Domain 4: Identity and Access Management

- Design and implement a scalable authorization and authentication system to access AWS resources.
- Understand the Principle of Least Privilege
- IAM Policies & Roles
- IAM JSON Policy Elements
- IAM Permission boundaries
- Understanding Delegation, STS
- Cross account policies & roles

- Understanding Federation & SSO
- AWS Directory services
- AWS Organizations
- S3 Security, Cross Account S3 access
- S3 Versioning
- AWS License manager
- AWS Cognito
- Troubleshoot an authorization and authentication system to access AWS resources

## Domain 5: Data Protection

- Design and implement key management and use
- Cryptography fundamentals
- Cloud Hardware Security Module (HSM)
- AWS Key Management Service (KMS)
- Envelope Encryption
- KMS Authentication and Access Control
- CloudTrail and Encryption
- EBS Architecture and Secure Data Wiping
- S3 Encryption
- Secrets Manager
- AWS Certificate Manager
- Load Balancer Security
- Docker and container security fundamentals
- AWS Glacier
- Troubleshoot key management.
- Design and implement a data encryption solution for data at rest and data in transit.

# Module 2 (Mapped to Azure AZ-500)

## 1. Azure Cloud Fundamentals

- Azure infrastructure: Regions, Availability Zones, Geographies
- Azure Resource Groups, Tags & ARM
- Azure Portal, Cloud Shell, Powershell and CLI
- Azure subscription
- Billing and cost management

## 2. Azure Virtual Machines

- Compile a checklist for creating an Azure Virtual Machine
- Describe the options available to create and manage an Azure Virtual Machine
- Availability management, Maintenance and Downtime
- Monitoring VMs
- Creating VM with Powershell/Bash
- Managing Linux Instances
- Availability Sets, Fault Domain and Update Domain
- VM Custom Script Extensions, DSC
- VM Scale Sets, Types scaling
- Azure Bastion Service
- Deploying ARN Templates
- Add Data Disks & NIC to VM
- Resizing VMs
- Azure disk encryption & Disk encryption on Windows
- VM security best practices
- Key vault for disk encryption
- VM backup & restore
- VM hardening in Security Center

## 3. Azure App Services

- Introduction to Azure app services
- App Service plans & sizing
- Web apps and settings
- Scalability

## 4. Containers & Security

- Containerization concepts, Docker & Kubernetes overview
- Azure Container Service (ACS)
- Azure Kubernetes Service (AKS)
- Create an AKS Cluster
- Create a container registry
- Run and application on Kubernetes
- Securing the container registry
- Container isolation for AKS
- Container security in AKS & Container scanning

## 5. Azure Storage Services

- Azure storage accounts overview
- Access Keys and Shared Access Signature (SAS)
- Storage Types, Standard & premium storage accounts
- Create Storage Account
- Azure Storage Explorer
- Azure Blob Containers
- Storage Performance Tiers
- Blob Access Policies
- Blob Storage Pricing
- Azure Files
- Files Vs Blobs
- Azure File Sync

- Secure File Transfer
- File Share Snapshots
- Storage Security & Authorization Options
- Storage Security, Encryption keys & Key Vault
- Managing Permissions
- Blob Public Access Level
- RBAC Authentication for Storage
- Log Analytics
- AZ Copy
- Azure Backup
- Azure Import/Export
- Azure CDN

## 6. Azure Virtual Network (Vnet)

- Purpose of Virtual Networks
- Creating a private network in Azure
- Subnets
- Azure Service Endpoints
- Domain and Custom Domains
- Azure DNS
- DNS Delegation
- Public and Private zones
- Network Security Groups
- Azure Load Balancing Services
- Azure Application Gateway
- Network Traffic Management & Network Routing
- User defined routes & Vnet peering
- Gateway Transit
- Virtual Network Gateway
- Azure firewall
- DDoS protection

## 7. Azure Active Directory

- Azure AD overview
- Create an Azure AD tenant
- AD Identity protection
- Conditional Access
- Managing Users, Groups & Devices
- Self Service Password Reset
- AD Connect, Hybrid Identities & identity protection
- SSO and MFA
- Managing Role Based Access Control
- Service principals
- App registration

## 8. Secure Access by using Azure AD (PIM and Tenant Security)

- Privileged Identity Management overview
- Monitor privileged access for Azure AD Privileged Identity Management (PIM)
- Configure Access Reviews Assigning resource roles (RBAC)
- PIM role activation

## 9. Governance and Role-based access control (RBAC)

- RBAC overview
- Implementing effective RBAC
- Configure subscription and resource permissions
- Configure resource group permissions
- Configure custom RBAC roles
- Identify the appropriate role
- Apply principle of least privilege
- Azure Policies
- Subscription policies
- Configure security settings by using Azure Policy

- Configure security settings by using Azure Blueprint
- Azure resource locks

## 10. Security Operations

- Azure Monitor and Alerts
- Log Analytics
- Azure Security Center
- Evaluate vulnerability scans from Azure Security Center
- Configure Just in Time VM access by using Azure Security Center
- Configure centralized policy management by using Azure Security Center
- Configure compliance policies and evaluate for compliance by using Azure Security Center
- Monitor Security by using Azure Sentinel
- Create and customize alerts
- Data sources for Azure Sentinel
- Evaluating results

## 11. Secure Data Services

- Azure Database services
- Azure SQL service
- SQL long term backup retention
- Azure SQL DB Advanced Threat Protection
- Database encryption
- Design auditing and caching strategies
- Azure Cosmos DB
- Azure Data Lake Store

## 12. Key Management

- Encryption and key management
- Azure Key Vault
- Manage permissions to secrets, certificates, and keys

- Configure RBAC usage in Azure Key Vault
- Configure key rotation

## Module 3 (Mapped to CCSP)

### Domain 1: Cloud Concepts, Architecture and Design

1.1 Understand Cloud Computing Concepts
1.2 Describe Cloud Reference Architecture
1.3 Understand Security Concepts Relevant to Cloud Computing
1.4 Understand Design Principles of Secure Cloud Computing
1.5 Evaluate Cloud Service Providers

### Domain 2: Cloud Data Security

2.1 Describe Cloud Data Concepts
2.2 Design and Implement Cloud Data Storage Architectures
2.3 Design and Apply Data Security Technologies and Strategies
2.4 Implement Data Discovery
2.5 Implement Data Classification
2.6 Design and Implement Information Rights Management (IRM)
2.7 Plan and Implement Data Retention, Deletion and Archiving Policies
2.8 Design and Implement Auditability, Traceability and Accountability of Data Events

### Domain 3: Cloud Platform and Infrastructure Security

3.1 Comprehend Cloud Infrastructure Components
3.2 Design a Secure Data Center
3.3 Analyze Risks Associated with Cloud Infrastructure
3.4 Design and Plan Security Controls
3.5 Plan Disaster Recovery (DR) and Business Continuity (BC)

## Domain 4: Cloud Application Security

4.1 Advocate Training and Awareness for Application Security

4.2 Describe the Secure Software Development Life Cycle (SDLC) Process

4.3 Apply the Secure Software Development Life Cycle (SDLC)

4.4 Apply Cloud Software Assurance and Validation

4.5 Use Verified Secure Software

4.6 Comprehend the Specifics of Cloud Application Architecture

4.7 Design Appropriate Identity and Access Management (IAM) Solutions

## Domain 5: Cloud Security Operations

5.1 Implement and Build Physical and Logical Infrastructure for Cloud Environment

5.2 Operate Physical and Logical Infrastructure for Cloud Environment

5.3 Manage Physical and Logical Infrastructure for Cloud Environment

5.4 Implement Operational Controls and Standards (e.g., Information Technology Infrastructure Library (ITIL), International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 20000-1)

5.5 Support Digital Forensics

5.6 Manage Communication with Relevant Parties

5.7 Manage Security Operations

## Domain 6: Legal, Risk and Compliance

6.1 Articulate Legal Requirements and Unique Risks within the Cloud Environment

6.2 Understand Privacy Issues

6.3 Understand Audit Process, Methodologies, and Required Adaptations for a Cloud Environment

6.4 Understand Implications of Cloud to Enterprise Risk Management

6.5 Understand Outsourcing and Cloud Contract Design

INFOSECTRAIN

sales@infosectrain.com | www.infosectrain.com