

AWS Security Specialty Training



CloudSiksha

AWS Security Specialty Certification

- Abilities Validated by the Certification
 - An understanding of specialized data classifications and AWS data protection mechanisms
 - An understanding of data encryption methods and AWS mechanisms to implement them
 - An understanding of secure Internet protocols and AWS mechanisms to implement them
 - A working knowledge of AWS security services and features of services to provide a secure production environment
 - Competency gained from two or more years of production deployment experience using AWS security services and features
 - Ability to make tradeoff decisions with regard to cost, security, and deployment complexity given a set of application requirements
 - An understanding of security operations and risk

Exam Content

Domain	% of Examination
Domain 1: Incident Response	12%
Domain 2: Logging and Monitoring	20%
Domain 3: Infrastructure Security	26%
Domain 4: Identity and Access Management	20%
Domain 5: Data Protection	22%
TOTAL	100%

About the Exam



Multi choice questions



Multiple response



65 questions in 170 minutes



Graded between 100 to 1000 marks



Pass marks is 750

Pre-requisite for this course



EC2



EBS



S3



VPC

AWS services covered in this course - 1

Guard Duty

IAM

System Manager Parameter Store

AWS Config

CloudWatch

VPC Flow Logs

S3 Event notification

Macie

Athena

AWS Services covered in this course - 2

AWS Organizations

CloudFront

Firewalls (SG, NACL, WAF)

VPC & VPN

API Gateway & Security

Lambda & Security

Amazon Cognito

IAM and S3

AWS Services covered in this course -3

Identity Federation

Cryptography

HSM

KMS

AWS Certificate Manager

AWS Secrets Manager

Encryption & AWS Services

Thanks



CloudSiksha