Auditing in AWS Cloud

1. Introduction to AWS Auditing (15 mins)

- Overview of AWS architecture
- Why auditing is crucial for AWS security
- Common AWS auditing standards (e.g., CIS benchmarks, NIST, ISO)

2. Governance in AWS (1 hour)

2.1 AWS Usage and Implementation (15 mins)

- Understanding AWS deployment models (Public, Private, Hybrid)
- Examples of typical AWS services used (EC2, S3, RDS)

2.2 Identifying Assets & Defining AWS Boundaries (10 mins)

- Identifying key AWS resources (EC2, S3, VPCs)
- Defining security perimeters and trust zones

2.3 Access Policies & Risk Management (15 mins)

- Overview of AWS Identity and Access Management (IAM)
- Implementing role-based access control (RBAC)
- Evaluating risk: Identifying, reviewing, and assessing AWS-related risks

2.4 Documentation and Inventory Management (10 mins)

- Using AWS Config and AWS Systems Manager for auditing inventory
- Best practices for tracking AWS resources

2.5 Adding AWS to Risk Assessments (5 mins)

- Integrating AWS risk into the broader organization risk management

2.6 IT Security and Program Policies (5 mins)

- Establishing AWS governance policies
- Aligning AWS usage with organizational security frameworks

3. Network Management and Security Controls (1 hour)

3.1 Network Security Controls in AWS (15 mins)

- Securing VPCs: NACLs, Security Groups
- Network segmentation and micro-segmentation

3.2 Physical Links and Environment Isolation (10 mins)

- Auditing physical security controls of AWS data centers
- Reviewing isolation of production and non-production environments

3.3 Granting and Revoking Access (10 mins)

- Implementing least privilege access in network management
- Periodic reviews and revoking unused access

3.4 DDoS Layered Defense (10 mins)

- AWS Shield, AWS WAF, and CloudFront integration for DDoS protection

3.5 Malicious Code Controls (10 mins)

- AWS tools for malware detection (GuardDuty, Inspector)

3.6 Documentation and Inventory for Network Components (5 mins)

- Auditing VPCs, subnets, and gateways

4. Security of AWS Console and API Access (30 mins)

4.1 Auditing AWS Console and API Access (10 mins)

- Monitoring console and programmatic access
- Best practices for AWS CloudTrail auditing

4.2 IPSec Tunnels and VPNs (10 mins)

- Securing and auditing VPN and Direct Connect

4.3 SSL Key Management and Protecting PINs at Rest (10 mins)

- Managing SSL certificates with AWS Certificate Manager (ACM)
- Data encryption methods for PINs and sensitive data

5. Logging and Monitoring in AWS (1 hour 15 mins)

5.1 Centralized Log Storage (15 mins)

- Implementing AWS CloudWatch Logs and S3 for log storage
- Reviewing logs from multiple accounts and regions

5.2 Reviewing Policies for Adequacy (10 mins)

- Ensuring logging policies meet organizational requirements
- Automating log reviews with AWS Lambda

5.3 Reviewing IAM Credentials Report (15 mins)

- Auditing IAM user credentials, access keys, and MFA configuration

5.4 Aggregating from Multiple Sources (10 mins)

- Using AWS CloudWatch, CloudTrail, and third-party tools for a holistic view

5.5 Intrusion Detection & Response (15 mins)

- AWS GuardDuty, AWS Macie, and AWS Security Hub

- Automating incident response using AWS Config and Lambda

---

6. Closing Q&A Session (15 mins)

- Address any additional questions
- Provide key takeaways and resources for future reference