**Day 2 - Identity & Access Management (IAM) (11.6.)**

**Day 2 – Access & Identity**

**1. IAM Deep Dive (AWS Focus)**

**Topics**

IAM core components: Users, Groups, Roles, Policies

MFA: Configuration and enforcement

Policy structure and evaluation logic (Allow vs. Deny, JSON syntax)

SCPs (Service Control Policies) in AWS Organizations

Temporary security credentials (STS, AssumeRole)

**Required Infrastructure & Components**

AWS Organization with multiple accounts (sandbox & prod)

IAM users and groups

IAM roles and role-based access control setup

Policies with scoped permissions (least privilege)

MFA-enforced accounts

**To-Dos & Steps**

Create users with custom policies for specific services (e.g., S3 admin, read-only EC2)

Set up roles for cross-account access

Enable and enforce MFA for console login

Apply SCPs to restrict certain services in child accounts

Use STS to demonstrate temporary credential usage

IAM Policy Simulator to test and debug policies

**Webinars**:

[AWS re:Inforce – Identity and Access Management Best Practices](https://aws.amazon.com/de/iam/resources/best-practices/)

Deep Dive on AWS IAM Policies Webinar - <https://www.youtube.com/watch?v=MKhkLqN0AyY> – 00:51

AWS Security Webinar: Getting Started with IAM - <https://aws.amazon.com/iam/getting-started/>

**YouTube**:

[AWS IAM Explained (Users, Groups, Roles)](https://www.youtube.com/watch?v=_ZCTvmaPgao) – 00:21

[AWS Organizations and SCPs Explained](https://www.youtube.com/watch?v=FR36p7iiRkU) – 00:07

[AWS STS (Security Token Service) Deep Dive](https://www.youtube.com/watch?v=dqF4VJCska4) – 00:15

**Reading Material**:

[AWS IAM User Guide](https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html)

[IAM Policy Reference Guide](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html)

[AWS Organizations Best Practices](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_best-practices.html)

[MFA in AWS Documentation](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html)

[AWS STS Concepts](https://docs.aws.amazon.com/STS/latest/APIReference/Welcome.html)

**2. GDPR Deep Dive (Compliance Focus)**

**Topics**

GDPR Key Principles:

Consent & Lawfulness

Data Minimization

Purpose Limitation

Rights of Data Subjects

Access Control from a GDPR perspective

Data Protection by Design & by Default

Logging and accountability obligations

**Required Infrastructure & Components**

IAM policies demonstrating least privilege

Audit logs via CloudTrail

AWS Config rules monitoring access control

KMS for encryption of personal data

S3 bucket with object-level access logging

**To-Dos & Steps**

Map IAM roles and policies to GDPR requirements (e.g., data minimization, access control)

Set up CloudTrail to monitor access to personal data

Configure Config rules to detect non-compliant access configurations

Use KMS with key policies to enforce access controls on sensitive datasets

Discuss real-world scenarios (e.g., employee access to EU customer data)

**Webinars**:

AWS Security and Compliance – Deep Dive into GDPR - <https://aws.amazon.com/de/blogs/security/a-deep-dive-into-data-protection-sessions-at-aws-reinforce-2025/>

[AWS – GDPR Compliance on AWS](https://docs.aws.amazon.com/whitepapers/latest/navigating-gdpr-compliance/welcome.html)

**YouTube**:

[AWS GDPR and Data Protection Explained](https://www.youtube.com/watch?v=s1e7_oh9dVk) – 00:28

[Data Privacy and GDPR for Cloud Professionals](https://www.youtube.com/watch?v=TTA_P3DDGmk) – 00:44

**Reading Material**:

[AWS GDPR Center](https://aws.amazon.com/compliance/gdpr-center/)

AWS Whitepaper: Navigating GDPR Compliance [Navigating GDPR Compliance on AWS - AWS Whitepaper](https://docs.aws.amazon.com/pdfs/whitepapers/latest/navigating-gdpr-compliance/navigating-gdpr-compliance.pdf) Compliance

[AWS Artifact for Compliance Documentation](https://aws.amazon.com/artifact/) – page 4-46

[AWS CloudTrail User Guide](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html), page 1-20

[AWS KMS Developer Guide](https://docs.aws.amazon.com/kms/latest/developerguide/overview.html)

[AWS Config Best Practices](https://docs.aws.amazon.com/config/latest/developerguide/best-practices.html)

**🎯End-of-Day Goal / Outcomes**

Participants should be able to:

Design and apply fine-grained IAM policies

Implement MFA and temporary credentials for secure access

Understand and map AWS access management practices to GDPR compliance requirements

Demonstrate how IAM, SCPs, and encryption contribute to secure identity and access management in a regulated environment