BLACKBIRD FOR TRAINING

IT Systems: Identity and Access Management

18 – 22 July 2027
Istanbul (Turkey)



IT Systems: Identity and Access Management

Ref: 321561_132658 **Date:** 18 – 22 July 2027 **Location:** Istanbul (Turkey) **Fees:** 4900 GBP



Introduction

In today's digital landscape, ensuring the security of information and systems is more critical than ever. This IT Identity and Access Management IAM course offers a deep dive into the world of information technology systems, helping professionals understand how to secure and manage access to critical IT systems effectively. The course is designed to be highly interactive, incorporating group discussions, case studies, and hands-on exercises that allow participants to apply their newfound knowledge in practical scenarios.

Through engaging role-playing and real-world case studies, participants will gain the expertise required to build, implement, and manage IT systems, particularly focusing on identity and access management IAM. This course will help you understand how to create secure IT infrastructures, manage user identities, and deploy access control mechanisms effectively.

Course Objectives

By the end of this course, participants will be able to:

- Illustrate IAM Architecture: Understand the IAM architecture framework and discuss the security risks associated with various deployment options in IT systems.
- Establish Strong Authentication Mechanisms: Learn the mechanisms for establishing strong authentication like OTP, certificate-based authentication, and device authentication.
- Explain Public Key Infrastructure: Understand the principles of Public Key Infrastructure PKI and certification authorities, and explore how they mitigate security risks in modern IT systems.
- Discuss Access Control Mechanisms: Learn about the most well-known access control mechanisms and how OAuth, OATH, SAML, and OpenID standards are applied in the IT identity and access management domain.
- Apply IAM with Practical Case Studies: Demonstrate the implementation of IAM using selected industrial tools through case studies e.g., e-passport, mobile banking, EMV schemes, and e-movement services.
- Explore IAM and Cloud Computing: Understand the role of IAM in cloud computing and its integration with various IT systems.



Course Outlines

Day 1: Introduction and Principles of Information Security

- Overview of Identity and Access Management IAM.
- Key attributes of information security systems.
- Principles of confidentiality, integrity, availability, non-repudiation, and accountability.
- The importance of auditability in managing IT systems.
- Symmetric and asymmetric cryptography, hashing, and digital signatures.
- Key management principles and techniques.

Day 2: Public Key Infrastructure PKI

- Understanding the architecture: certification and registration authorities.
- Life cycle management of digital certificates.
- Types of certificates and their usage patterns.
- Exploring encryption, digital signatures, and client certificates.
- Case studies: Email protection, mobile banking, and document signing.

Day 3: Identification and Authentication

- Overview of identification, verification, and authentication.
- Various mechanisms for identity authentication such as One-Time Passwords OTP, biometrics, smart cards, and soft tokens.
- Risk-based authentication and step-up authentication.
- Implementing Single Sign-On SSO and federated SSO.
- Key IAM frameworks and industrial tools.
- Understanding security risks in authentication mechanisms.

Day 4: Access Control

- Principles of authorization and various access control schemes.
- Understanding OAuth protocol and its application in modern IT systems.
- Overview of enterprise rights management and digital rights management DRM.
- Privileged account management: Managing access to sensitive resources.
- Compliance and governance in IT access management.

Day 5: IAM Framework and Use Cases

- Detailed understanding of IAM architecture framework.
- IAM ecosystem and its integration with cloud computing.
- Use cases and practical applications:
    - Border control, e-passports, national IDs.
    - E-banking and e-health systems.



Why Attend This Course: Wins & Losses!

- In-depth knowledge of IAM architecture and security risks, essential for the modern IT systems landscape.
- Practical understanding of strong authentication mechanisms, empowering you to create secure identity management systems.
- Expertise in Public Key Infrastructure PKI and how it helps mitigate risks in IT access management.
- Familiarity with key access control mechanisms and the role of standards like OAuth, OATH, SAML, and OpenID in identity and access management.
- Hands-on experience in implementing IAM systems, helping you manage and safeguard your organization's IT systems effectively.
- Knowledge of IAM in cloud computing and practical case studies showcasing real-world applications.

Conclusion

This IT Identity and Access Management IAM course is an essential step for professionals looking to master the security and management of IT systems. With practical case studies, hands-on exercises, and a focus on strong authentication mechanisms, PKI, and access control, you will be equipped to design, implement, and manage IAM systems efficiently.

Gain critical skills to protect your organization's IT infrastructure and become a leader in identity and access management within your field. Don't miss the opportunity to enhance your expertise in IT systems and ensure the security of your enterprise.

