



IT074: IT Systems: Identity and Access Management





Training Description:

We are living in the age of the Internet of Things (IoT) which provides seamless integration and ease of access between various objects regardless of their physical proximity. The IoT is spreading across different vertical domains such as healthcare systems, government services, banks and telecommunications, just to name a few. We are no longer only vulnerable to attacks against valuable enterprises' digital content but also to life threatening attacks, terrorist attacks, espionage attacks, etc. The need for providing identity assurance and stringent access control, as a result, is of utmost importance.

This intensive training course covers the fundamental principles and architecture framework for an end-to-end IT identity and access management system. This includes identity assurance, authentication, authorization, accountability, auditability, Single Sign-On (SSO) and identity federation. It also discusses practical case studies such as e-passport, mobile banking, e-government services, EMV systems and other selected cases.

Training Objectives:

By the end of the training, participants will be able to:

- ✓ Illustrate the identity and access management architecture framework and discuss the security risks associated with its various deployment options
- ✓ Discuss the different mechanisms for establishing strong authentication (e.g. OTP, certificate based authentication, device authentication, etc.)
- ✓ Explain the principles of key public infrastructure and certification authorities, and demonstrate their value in mitigating the security risks facing modern societies
- ✓ Explain the most well-known access control mechanisms and the roles of oauth, OATH, SAML and OpenID standards in the IAM domain and apply the concepts of (federated) SSO
- ✓ Demonstrate the building of IAM using selected industrial tools and practical case studies (e.g. e-passport and boarder gate, mobile-banking, EMV scheme, and e-movement services)

Training Designed for:

This intensive course is intended for IT professionals such as IT Strategic Planners, Project Managers, Security Managers, Security Architects and Risk Managers. Although the course is technical in nature, complex concepts are discussed at an abstract level to fit the needs of participants from various technical backgrounds.

Target Competency:

- Project management
- Information security management
- Implementing public key infrastructure
- Identification and authentication management
- Identity Access Management (IAM)

Training Requirement:

“Hand’s on practical sessions, equipment and software will be applied during the course if required and as per the client’s request.” **Practical sessions** will be organized during the course for participants to practice the theory learnt.



Please note that the below **topics can be amended as per client's learning needs and objectives**. Further, it should be forwarded to us a month prior to the course dates.

Training Program:

FIVE DAYS:

- ❖ PRE-TEST
- ❖ Introduction and principles of information security:
 - Identity and access management (IAM) overview
 - Attributes of information security:
 - Confidentiality
 - Integrity
 - Availability
 - Non-repudiation
 - Accountability
 - Auditability
 - Symmetric and asymmetric cryptography
 - Hashing and digital signature
 - Key management
- ❖ Public Key Infrastructure (PKI)
 - Architecture: certification and registration authority
 - Life cycle management
 - Types of certificates and usage patterns
 - Encryption
 - Digital signature
 - Client certificate
 - SSL server certificate
 - Attribute based certificate
 - Case studies (e.g. email protection, mobile banking, and document signing)
- ❖ Identification and authentication
 - Identification, verification and authentication overview
 - Mechanisms of identification and authentication
 - Onetime password
 - Biometric
 - Digital signature
 - Smartcard
 - Soft/hard tokens
 - Mobile device
 - Risk based authentication
 - Step-up authentication
 - Single-sign on and federated single-sign-on
 - OATH, OpenID, BorwserID, and SAML
 - Architecture framework and industrial tools
 - Trusted computing role in identity assurance



- Security risks associated with the discussed mechanisms
- ❖ **Access control**
 - Principles of authorization
 - Access control schemes
 - OAuth protocol
 - Enterprise rights management and digital rights management
 - Privileged account management
 - Governance and compliance
- ❖ **IAM framework and use cases**
 - IAM architecture framework
 - IAM echo system
 - IAM and cloud computing
 - Illustrative use cases
 - Border control
 - E-passport
 - National ID
 - E-banking
 - E-health system
 - EMV scheme
- ❖ **Course Conclusion**
- ❖ **POST-TEST and EVALUATION**

Training Methodology:

This course is highly interactive and includes group discussions, case studies and syndicate work. It also includes practical exercises and role playing that allow all participants to use the knowledge they gained to demonstrate their skills in identity and access management.

This interactive virtual training course includes the following training methodologies as a percentage of the total tuition hours:-

- 30% Lectures, Concepts, Role Play
- 70% Workshops & Work Presentations, Techniques, Based on Case Studies & Practical Exercises, Software & General Discussions
- Pre and Post Test

Training Certificate(s):

Internationally recognized certificate will be issued to each participant who completed the course

Training Fees:

As per the course location - This rate includes participant's manual, hand-outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Note: The 5% VAT (Value Added Tax), will be effective starting 01st of January 2018 as per the new regulation from the UAE Government. The VAT applies for all quotation both for local and abroad.





Training Timings:

Daily Timings:

07:45 - 08:00	Morning Coffee / Tea
08:00 - 10:00	First Session
10:00 - 10:20	Recess (Coffee/Tea/Snacks)
10:20 - 12:20	Second Session
12:20 - 13:30	Recess (Prayer Break & Lunch)
13:30 - 15:00	Last Session

For training registrations or in-house enquiries, please contact:

Aisha Relativo: aisha@cmc-me.com

Tel.: +971 2 665 3945 or +971 2 643 6653 | Mob.: +971 52 2954615

Training & Career Development Department

