

# USER ACCOUNT MANAGEMENT AUDIT: ASSESSES THE PROCESSES FOR CREATING, MODIFYING, AND DEACTIVATING USER ACCOUNTS

*“Ensuring Secure and Efficient User Account Lifecycle Management”*

## Schedule

Date	Venue	Fees (Face-to-Face)
20- 24 Jul 2026	London, UK	USD 3495 per delegate

▶ **Available delivery methods:** Face-to-Face & Online Training

## Introduction

User account management is a critical element of an organization’s overall security strategy. Proper processes for creating, modifying, and deactivating user accounts help prevent unauthorized access, ensure compliance, and safeguard sensitive information. This course will explore the essential aspects of user account management auditing, focusing on best practices, policies, and tools for monitoring user account activities and ensuring they are properly managed throughout their lifecycle. Participants will gain hands-on experience in auditing user accounts, assessing risks, and applying solutions to strengthen account management processes.

The course will dive into the technical and procedural elements of user account management, covering the full spectrum of account lifecycle processes, from creation to termination. By the end of this training, participants will be able to identify potential vulnerabilities in account management systems and apply auditing techniques to mitigate risks and ensure compliance with industry standards and regulations.

## Objectives

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

- Understand the fundamental principles of user account management and its significance in cybersecurity
- Audit user account management processes, including creation, modification, and deactivation
- Identify vulnerabilities in user account systems and recommend effective corrective measures
- Assess compliance with internal security policies and external regulatory requirements
- Implement best practices for ensuring secure and efficient user account management

## Why Attend

- Gain expertise in auditing user account management processes to enhance security
- Learn how to identify risks and vulnerabilities in user account systems
- Understand industry standards and best practices for user account lifecycle management
- Enhance your organization's security posture by ensuring compliance with account management policies
- Improve your auditing skills with practical case studies and hands-on exercises

## Target Audience

This program is designed for:

- IT auditors and security professionals
- System administrators responsible for user account management
- Compliance officers and data protection officers
- Cybersecurity professionals focusing on identity and access management
- Risk management professionals
- IT managers and directors overseeing user account and access control systems

## Individual Benefits

Key competencies that will be developed include:

- Proficiency in auditing user account management practices
- Ability to identify and mitigate risks associated with user accounts
- Knowledge of regulatory compliance requirements related to account management
- Enhanced ability to apply security best practices to account lifecycle management
- Capability to recommend improvements to strengthen user access control and account management policies

## Organizational Benefits

Upon completing the training course, participants will demonstrate:

- The ability to conduct thorough audits of user account management systems
- Improved security posture by identifying and addressing user account management vulnerabilities
- Enhanced understanding of regulatory compliance requirements and how to maintain it
- Capability to implement stronger controls over user accounts and reduce the risk of unauthorized access
- Expertise in maintaining a secure and efficient user account lifecycle process

## Instructional Methodology

The course follows a blended learning approach combining theory with practice:

- Strategy Briefings – Overview of user account management and security policies
- Case Studies – Real-world examples of security breaches due to improper user account management
- Workshops – Hands-on exercises to audit user accounts and apply corrective actions
- Peer Exchange – Group discussions on best practices and lessons learned from past audits
- Tools – Templates for user account audits, reporting, and security assessment

## MAWA EVENTS

**Address:** No. 857, Block A2, Leisure Commerce Square - No 9., 46150 Petaling Jaya, Selangor, Malaysia

**Phone:** +601116373203 | **Email:** info@mawaevents.net

---



## Course Outline

### Detailed 5-Day Course Outline

**Training Hours:** 7:30 AM – 3:30 PM **Daily Format:** 3–4 Learning Modules | Coffee breaks: 09:30 & 11:15 | Lunch Buffet: 01:00 – 02:00

#### Day 1: Introduction to User Account Management and Security

- Module 1: Fundamentals of User Account Management (07:30 – 09:30)
  - Overview of user account management lifecycle
  - Key principles of identity and access management (IAM)
  - Importance of account management in cybersecurity
- Module 2: The User Account Lifecycle (09:45 – 11:15)
  - Processes of account creation, modification, and deactivation
  - Risks associated with each stage of the account lifecycle
  - Best practices for secure account management
- Module 3: Regulatory Requirements and Compliance (11:30 – 01:00)
  - Overview of relevant regulations (GDPR, HIPAA, etc.)
  - Compliance requirements for user account management
  - How to align user account management processes with regulatory standards

#### Day 2: Auditing User Account Management Practices

- Module 4: Planning and Conducting User Account Audits (07:30 – 09:30)
  - Key steps in auditing user account management processes
  - Tools and techniques for effective auditing
  - Common challenges faced in user account audits
- Module 5: Detecting Vulnerabilities in User Account Management (09:45 – 11:15)
  - Identifying common vulnerabilities and weaknesses in account management
  - Methods for auditing access control systems
  - Conducting risk assessments for user accounts
- Module 6: Case Study: Real-World User Account Breaches (11:30 – 01:00)
  - Review of high-profile incidents involving compromised user accounts
  - Lessons learned from security breaches
  - Best practices for mitigating risks and vulnerabilities

#### Day 3: Advanced Techniques in User Account Auditing

- Module 7: Auditing Privileged User Accounts (07:30 – 09:30)
  - Special considerations for privileged and administrative accounts
  - Auditing access to sensitive systems and data
  - Implementing least privilege principles
- Module 8: User Authentication and Access Control (09:45 – 11:15)
  - Best practices for user authentication (password policies, MFA, etc.)
  - Audit techniques for ensuring secure authentication processes
  - Access control models and their impact on user account security
- Module 9: Reporting and Documentation for Audits (11:30 – 01:00)
  - Creating audit reports and documenting findings
  - Presenting audit results to senior management
  -

Developing corrective action plans based on audit findings

**Day 4: Remediation and Security Improvements**

- Module 10: Corrective Actions for Weaknesses Identified in Audits (07:30 – 09:30)
- Developing and implementing action plans to address vulnerabilities
- Working with IT teams to resolve identified issues
- Monitoring the effectiveness of remediation efforts
- Module 11: Enhancing Security Controls for User Accounts (09:45 – 11:15)
- Strengthening access controls and account management policies
- Implementing automated tools for account lifecycle management
- Continuous monitoring and improvement strategies
- Module 12: Workshop: Conducting a Full User Account Audit (11:30 – 01:00)
- Hands-on exercise to perform a user account audit on a sample system
- Identifying vulnerabilities and proposing solutions
- Group discussion and feedback on audit results

**Day 5: Final Assessment and Certification**

- Module 13: Final Review and Q&A (07:30 – 09:30)
- Recap of key learning points and best practices
- Open session for questions and answers
- Module 14: Group Exercise: Creating an Audit Plan for User Account Management (09:45 – 11:15)
- Group activity to create a detailed user account audit plan
- Presentations and feedback from peers
- Module 15: Certification and Closing Remarks (11:30 – 01:00)
- Distribution of certificates of completion
- Final remarks and steps for applying the learning in the workplace

**Certification**

Participants will receive a Certificate of Completion in User Account Management Auditing, validating their ability to assess and improve user account management processes, enhance security controls, and ensure compliance with industry standards and regulatory requirements.

**Why Choose MAWA Events**

- **Global Expertise:** More than 17 years of experience in professional training and consulting.
- **Industry-Leading Faculty:** Courses delivered by seasoned professionals with hands-on experience.
- **Practical Insights:** Learn to turn theory into actionable strategies for real-world business impact.
- **Client-Focused Solutions:** Customized programs designed to achieve your organisation's unique goals.

**In-House / Customized Training**

Interested in running this course for your team?

Please contact us:

TEL:

**+601116373203**

EMAIL:

**info@mawaevents.net**

© Material published by MAWA Events shown here is copyrighted. All rights reserved. Any unauthorized copying, distribution, use, dissemination, downloading, storing (in any medium), transmission, reproduction or reliance in whole or any part of this course outline is prohibited and will constitute an infringement of copyright.