

CYBER SECURITY IN ACCOUNTING & FINANCIAL MANAGEMENT

“Enhancing Financial Security: Safeguarding Accounting Systems Against Cyber Threats”

Schedule

Date	Venue	Fees (Face-to-Face)
03 – 07 Aug 2026	London - UK	USD 3495 per delegate

► Available delivery methods: Face-to-Face & Online Training

Introduction

As the financial sector increasingly adopts digital systems for accounting and financial management, the need to protect these systems from cyber threats has never been greater. This 5-day intensive training course focuses on the intersection of cybersecurity and financial management, providing professionals with the tools to safeguard accounting data, financial transactions, and financial reporting systems from cyber threats.

Participants will explore the vulnerabilities unique to accounting and financial management systems, along with practical strategies for securing sensitive data. Through real-world case studies and hands-on exercises, you will learn how to implement robust cybersecurity measures to protect financial integrity, ensure compliance, and avoid the risks of financial fraud.

Objectives

- By the end of this course, participants will be able to:
- Understand the principles and best practices for securing accounting and financial management systems
 - Identify common cyber threats and vulnerabilities in the financial sector
 - Implement effective cybersecurity measures to protect sensitive financial data
 - Ensure compliance with cybersecurity regulations in the financial industry
 - Develop and maintain secure financial reporting processes
 - Design incident response plans for cyber threats and breaches in financial systems

Why Attend

- Gain a comprehensive understanding of cybersecurity risks specific to accounting and financial management
- Learn how to protect sensitive financial data from hacking, fraud, and cyber-attacks
- Discover how to implement security measures that comply with industry standards and regulations
- Improve your ability to respond to cyber incidents and minimize financial and reputational damage
- Enhance your career prospects by gaining expertise in a critical area of financial management
- Collaborate with peers in the financial and cybersecurity sectors to share experiences and insights

Target Audience

This program is designed for:

- Financial managers and accountants responsible for maintaining secure financial systems
- IT professionals working in the finance sector with an interest in cybersecurity
- Internal auditors and compliance officers who need to understand financial data protection
- Risk managers and professionals responsible for identifying and mitigating cybersecurity threats
- Consultants and advisors working with accounting or financial institutions

Individual Benefits

Key competencies that will be developed include:

- Enhanced understanding of cybersecurity challenges in accounting and financial systems
- Skills to identify and mitigate security risks in financial software and transactions
- Knowledge of compliance standards for financial cybersecurity
- Practical experience in creating and implementing cybersecurity strategies for financial data protection
- Proficiency in incident response planning and disaster recovery for financial systems

Organizational Benefits

Upon completing the training course, participants will demonstrate:

- The ability to protect financial data and accounting systems from cyber threats
- Knowledge of securing digital financial transactions and reporting systems
- Enhanced compliance with cybersecurity regulations in the financial sector
- The ability to develop and implement an organization-wide cybersecurity strategy for financial management
- Increased resilience to financial fraud and cyber-attacks, reducing potential financial and reputational damage

Instructional Methodology

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

- Strategy Briefings – Introduction to the principles of cybersecurity in accounting and financial management
- Case Studies – Real-world examples of cybersecurity breaches in financial systems and lessons learned
- Workshops – Hands-on exercises for securing financial data, systems, and transactions
- Peer Exchange – Group discussions on cybersecurity challenges and best practices in financial sectors
- Tools – Templates for risk assessments, cybersecurity policies, and incident response plans

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 Cybersecurity in Financial Systems

- Module 1: Overview of Cybersecurity in Financial Management (07:30 – 09:30)
 - Introduction to the principles of cybersecurity in accounting and financial systems
 - Key threats and vulnerabilities in financial systems
 - The role of cybersecurity in ensuring financial integrity and trust
- Module 2: Types of Cyber Threats in Accounting & Financial Systems (09:45 – 11:15)
 - Cyber-attacks commonly targeting accounting and financial software
 - Identifying threats like ransomware, phishing, and insider threats
 - How these threats affect financial data, transactions, and reporting
- Module 3: Cybersecurity Best Practices for Financial Data Protection (11:30 – 01:00)
 - Encryption and secure communication methods for financial transactions
 - User authentication and access control in accounting systems
 - Securing financial data both on-premise and in the cloud

Day 2: Regulatory Compliance and Financial Cybersecurity Standards

- Module 4: Compliance Regulations and Standards in the Financial Sector (07:30 – 09:30)
 - Key cybersecurity regulations affecting the financial industry (e.g., GDPR, PCI DSS)
 - Legal requirements for data protection and financial reporting
 - Auditing and compliance in the cybersecurity space
- Module 5: Cybersecurity Policies and Frameworks for Financial Systems (09:45 – 11:15)
 - Developing cybersecurity policies for accounting and financial institutions
 - Overview of cybersecurity frameworks and standards (e.g., NIST, ISO 27001)
 - Best practices for integrating cybersecurity policies within accounting processes
- Module 6: Internal Controls and Financial System Security (11:30 – 01:00)
 - Designing internal controls to prevent fraud and financial misreporting
 - Establishing secure financial reporting workflows
 - Role of auditors in ensuring cybersecurity compliance

Day 3: Cybersecurity Tools and Technologies for Financial Management

- Module 7: Security Tools for Protecting Financial Systems (07:30 – 09:30)
 - Overview of cybersecurity tools for securing financial data
 - Firewalls, antivirus software, and intrusion detection systems (IDS)
 - Implementing multi-factor authentication and role-based access control (RBAC)
- Module 8: Digital Transaction Security (09:45 – 11:15)
 - Securing financial transactions, both online and offline
 - Blockchain technology and its role in securing financial transactions
 - Preventing and responding to financial fraud in digital payments
- Module 9: Incident Detection and Response in Financial Systems (11:30 – 01:00)
 - How to identify signs of a cyber-attack in financial systems
 - Developing incident detection and monitoring strategies
 -

Steps to take in the event of a cyber incident or breach

Day 4: Case Studies, Risk Management, and Incident Response

- Module 10: Case Studies of Cyber Attacks on Financial Systems (07:30 – 09:30)
- Review of high-profile cyber-attacks on financial institutions
- Lessons learned from past breaches and cybersecurity failures
- Analysis of financial system vulnerabilities exposed in cyber-attacks
- Module 11: Risk Management for Cybersecurity in Financial Systems (09:45 – 11:15)
- Identifying, assessing, and mitigating risks in financial systems
- How to create a cybersecurity risk management plan for accounting operations
- Integrating risk management strategies into business continuity planning
- Module 12: Cybersecurity Incident Response and Disaster Recovery (11:30 – 01:00)
- Creating an incident response plan for cyber-attacks in financial systems
- Best practices for disaster recovery in financial organizations
- Conducting cybersecurity drills and simulations for financial institutions

Day 5: Final Review, Certification, and Action Plan Development

- Module 13: Review of Key Concepts (07:30 – 09:30)
- Recap of the cybersecurity measures discussed throughout the course
- Key strategies for securing financial systems and protecting sensitive data
- Module 14: Action Plan Development for Financial Cybersecurity (09:45 – 11:15)
- Participants will develop an action plan for implementing cybersecurity measures in their own financial systems
- Group discussions and peer feedback on proposed action plans
- Module 15: Certification and Closing (11:30 – 01:00)
- Certification ceremony
- Final Q&A and closing remarks

Certification

Participants will receive a Certificate of Completion in Cyber Security for Accounting & Financial Management, validating their expertise in securing financial systems, protecting sensitive data, and ensuring compliance with industry cybersecurity standards.

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

Follow us:  Facebook  Twitter  YouTube  LinkedIn  Instagram

© 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.