Cyber Security Risk Assessment & Management Masterclass

29 March – 2 April 2027
London (UK)

UK Traininig
PARTNER



Cyber Security Risk Assessment & Management Masterclass

Ref: 321388_158049 **Date:** 29 March – 2 April 2027 **Location:** London (UK) **Fees:** 6100 GBP

Why This Course

As organizations increasingly rely on digital systems, the scale and sophistication of cyber threats continue to rise. Cybersecurity risk management has become a strategic imperative — not only to protect data and operations, but also to sustain trust, comply with regulations, and ensure business continuity. Professionals equipped with the right frameworks and analytical skills can significantly strengthen organizational resilience against emerging cyber risks.

The Cybersecurity Risk Management & Threat Mitigation Executive Program is an intensive 1-week training designed for cybersecurity professionals, IT managers, auditors, compliance officers, and leaders seeking to master risk assessment and mitigation practices. Blending global frameworks with real-world applications, this program develops the skills needed to identify vulnerabilities, evaluate risks, implement controls, and effectively communicate cyber threats across the organization.

What You'll Learn and Practice

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

- Apply leading cybersecurity risk management frameworks NIST, ISO 27001, FAIR
- Conduct end-to-end cyber risk assessments and perform effective threat modeling
- Develop and deploy risk mitigation strategies aligned with business goals
- Build and maintain a robust cybersecurity governance and monitoring program
- Communicate cyber risks to stakeholders with clarity and confidence
- Strengthen overall organizational resilience through proactive risk practices

The Program Flow

Day 1 - Foundations of Cyber Risk Management

- Introduction to cybersecurity risk management concepts
- Overview of major frameworks: NIST RMF, ISO 27001, FAIR
- Understanding the global threat landscape and attack vectors
- Identifying, classifying, and prioritizing critical assets



Day 2 - Risk Assessment Methodologies

- Qualitative vs. quantitative risk assessment approaches
- Threat modeling techniques STRIDE, MITRE ATT&CK, kill chain analysis
- Vulnerability assessment and exploitation considerations
- Performing scenario-based risk assessments for realistic threats

Day 3 - Risk Mitigation Strategies

- Selecting and implementing appropriate security controls
- Applying risk treatment strategies: accept, avoid, transfer, mitigate
- Conducting cost-benefit and risk-reduction analyses
- Developing actionable risk mitigation and remediation plans

Day 4 - Continuous Monitoring & Incident Response

- Designing continuous monitoring programs and operational dashboards
- Key risk indicators KRIs, metrics, and reporting structures
- Incident response planning, execution, and post-incident review
- Business continuity planning BCP and disaster recovery DR strategies

Day 5 - Governance & Communication

- Building cybersecurity governance structures and policies
- Effective risk reporting using dashboards and executive summaries
- Communicating risks to senior leadership and boards
- Fostering a culture of cybersecurity awareness across the organization

Individual Impact

Participants will leave the program with:

- The capability to conduct comprehensive, accurate cyber risk assessments
- Practical skills to design and implement mitigation strategies
- Knowledge to establish a continuous monitoring and incident response framework
- Strong communication tools for articulating cyber risks to both technical and non-technical audiences
- Increased confidence in leading cybersecurity initiatives and decision-making

Organizational Impact

Organizations will benefit through:



- Enhanced cyber resilience and reduced exposure to security breaches
- Stronger alignment between cybersecurity practices and business objectives
- Improved governance, documentation, and compliance posture
- Faster, more accurate detection and response to cyber threats
- A culture of heightened security awareness and shared responsibility

Training Methodology

The program incorporates:

- Real-world case studies and cyber incident simulations
- Framework-based workshops and hands-on assessment exercises
- Group discussions, threat modeling labs, and collaborative problem-solving
- Practical templates, checklists, and tools for immediate workplace use
- Expert-led sessions linking cybersecurity theory with operational execution

Beyond the Course

Participants will return ready to:

- Lead cybersecurity risk assessments and strategic mitigation efforts
- Develop organizational policies and governance structures
- Support leadership with clear, data-backed cyber risk insights
- Strengthen defenses through continuous monitoring and incident readiness
- Advance cybersecurity maturity across their teams and organizations

