Cybersecurity Risk Management in the Digital Information Age

31 January – 4 February 2027
Cairo (Egypt)

UK Traininig
PARTNER



Cybersecurity Risk Management in the Digital Information Age

Ref: 322399_198031 **Date:** 31 January – 4 February 2027 **Location:** Cairo (Egypt) **Fees:** 4900 GBP

Why This Course

Cybersecurity risk management has become a critical priority for organizations operating in today's digital environment. As cyber threats continue to evolve, businesses need professionals who can identify risks, assess vulnerabilities, implement effective controls, and respond confidently to incidents before they cause serious operational, financial, or reputational damage.

This intensive 1-week Cybersecurity Risk Management Training program equips participants with the knowledge and practical skills needed to manage cyber risks from both technical and managerial perspectives. The course covers threat intelligence, vulnerability assessment, cybersecurity controls, incident response, crisis management, governance, compliance, and awareness culture. Through practical exercises, case discussions, and cyber attack simulations, participants will learn how to protect organizational assets and strengthen cyber resilience.

What You'll Learn and Practice

By joining this program, you will:

- Understand the current cybersecurity threat landscape and its business impact.
- Identify cyber risks, vulnerabilities, and potential attack scenarios.
- Apply cybersecurity risk management principles and best practices.
- Use cybersecurity frameworks to guide risk assessment and control implementation.
- Conduct vulnerability assessments and prioritize risks effectively.
- Classify assets and understand their role in cybersecurity planning.
- Implement security controls for networks, data, access, identity, and cloud environments.
- Develop cybersecurity policies, procedures, and risk mitigation strategies.
- Build incident response plans and manage cyber crisis situations.
- Understand legal, regulatory, and compliance requirements in cybersecurity.
- Promote cybersecurity awareness and strengthen organizational security culture.
- Measure and report cybersecurity effectiveness to stakeholders.



The Program Flow

Day 1: Introduction to Cybersecurity Risk Management

- Explore the current cybersecurity landscape and emerging threat patterns.
- Understand cyber risks and their impact on business operations.
- Learn the principles of risk management in cybersecurity.
- Review cybersecurity frameworks, standards, and best practices.
- Connect cybersecurity risk management with organizational resilience and business continuity.

Day 2: Threat Intelligence and Vulnerability Assessment

- Identify and analyze common cyber threats and attack methods.
- Understand how threat intelligence supports proactive risk management.
- Conduct vulnerability assessments across systems, networks, and processes.
- Apply asset management and classification techniques.
- Quantify, prioritize, and document cybersecurity risks for action planning.

Day 3: Cybersecurity Controls and Implementation

- Understand network security architecture and control design.
- Apply data protection strategies for sensitive and critical information.
- Implement access control and identity management practices.
- Explore cloud security risks, controls, and implementation considerations.
- Develop practical cybersecurity policies and procedures aligned with organizational needs.

Day 4: Incident Response and Crisis Management

- Develop structured incident response plans and escalation procedures.
- Participate in cyber attack simulations and tabletop exercises.
- Apply crisis communication strategies during cybersecurity incidents.
- Coordinate roles and responsibilities during incident response.
- Link incident response with business continuity and disaster recovery planning.

Day 5: Governance, Compliance, and Culture

- Understand cybersecurity governance and leadership responsibilities.
- Explore legal and regulatory compliance requirements in cybersecurity.
- Build strategies for fostering a culture of cybersecurity awareness.
- Measure and report cybersecurity performance and control effectiveness.
- Develop continuous improvement approaches for cybersecurity risk management.



Individual Impact

- Build confidence in identifying, assessing, and managing cybersecurity risks.
- Strengthen understanding of cybersecurity governance, controls, and compliance.
- Improve practical skills in vulnerability assessment and risk prioritization.
- Gain the ability to support or lead incident response efforts.
- Develop stronger awareness of cybersecurity leadership and communication practices.

Work Impact

- Improve organizational readiness against cyber threats and attacks.
- Strengthen cybersecurity policies, procedures, and control environments.
- Reduce exposure to operational, financial, legal, and reputational cyber risks.
- Improve incident response coordination and crisis management capability.
- Promote a stronger cybersecurity culture across teams and departments.

Training Methodology

This program combines cybersecurity risk concepts with practical application through:

- Real-world cyber risk case studies and scenario discussions.
- Vulnerability assessment and risk prioritization exercises.
- Cybersecurity policy and procedure development workshops.
- Cyber attack simulations and tabletop incident response activities.
- Governance, compliance, and reporting practice sessions.
- Group discussions on cybersecurity culture, awareness, and continuous improvement.

Beyond the Course

Upon completion, participants will be able to:

- Conduct comprehensive cybersecurity risk assessments.
- Identify vulnerabilities and prioritize cyber risks based on business impact.
- Develop and implement effective cybersecurity policies and procedures.
- Apply suitable security controls to protect organizational assets.
- Lead or support incident response efforts during cyber attacks.
- Promote cybersecurity awareness and contribute to a stronger security culture.

