BLACKBIRD FOR TRAINING

Cybersecurity Risk Management and Incident Response

11 – 15 January 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER



www.blackbird-training.com

Cybersecurity Risk Management and Incident Response

Ref: 3255743_350091 **Date:** 11 – 15 January 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

The Cybersecurity Risk Management and Incident Response course focuses on managing cyber risks and responding to security incidents in a structured and practical way. Organizations face increasing threats that may affect data, systems, operations, reputation, and service continuity. Effective cybersecurity management requires risk identification, control assessment, incident readiness, response coordination, and continuous improvement.

This course explains how to identify cybersecurity risks, assess their impact, prioritize controls, prepare incident response plans, and manage incidents from detection to recovery. It also covers communication during incidents, documentation, lessons learned, and the connection between risk management, compliance, and operational resilience.

The course is delivered over five connected days. It begins with cybersecurity risk foundations, then moves into risk assessment and control planning, incident response preparation, incident handling and recovery, and finally performance review and continuous improvement. The content is aligned with the provided course topic.

Course Objectives

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

- Understand the principles of cybersecurity risk management.
- Identify key cyber threats, vulnerabilities, and business impacts.
- Assess and prioritize cybersecurity risks.
- Link cybersecurity risks with operational, compliance, and reputational consequences.
- Evaluate existing controls and identify gaps.
- Develop practical cybersecurity risk treatment actions.
- Prepare structured incident response plans.
- Define roles, responsibilities, and escalation paths during incidents.
- Manage incident detection, containment, eradication, and recovery.
- Document incidents and collect required evidence.
- Communicate effectively with relevant stakeholders during incidents.
- Review incident outcomes and improve cyber resilience.



Course Outlines

Day 1: Foundations of Cybersecurity Risk Management.

- Concept of cybersecurity risk and its business impact.
- Common cyber threats affecting organizations.
- Relationship between assets, threats, vulnerabilities, and controls.
- Difference between risk prevention, detection, response, and recovery.
- Cybersecurity roles and responsibilities across departments.
- Key challenges in managing cybersecurity risks.

Day 2: Cyber Risk Assessment and Control Planning.

- Identifying critical assets and information systems.
- Assessing threats, vulnerabilities, likelihood, and impact.
- Prioritizing risks based on business consequences.
- Reviewing existing security controls.
- Identifying gaps in protection, monitoring, and response readiness.
- Practical application of preparing a cyber risk register.

Day 3: Incident Response Planning and Readiness.

- Purpose of an incident response plan.
- Defining incident categories, severity levels, and escalation rules.
- Building the incident response team structure.
- Preparing communication and reporting procedures.
- Coordinating with information technology, legal, compliance, and management teams.
- Practical application of preparing an incident response plan outline.

Day 4: Incident Handling, Containment, and Recovery.

- Detecting and validating cybersecurity incidents.
- Containing incidents to reduce operational impact.
- Investigating root causes and affected systems.
- Eradicating threats and restoring services.
- Documenting actions, timelines, decisions, and evidence.
- Practical application of managing a cybersecurity incident scenario.



Day 5: Lessons Learned and Continuous Improvement.

- Reviewing incident response performance.
- Identifying control weaknesses and response gaps.
- Preparing lessons learned reports.
- Updating risk registers and response plans.
- Measuring cybersecurity readiness and resilience.
- Integrated application linking risk assessment, controls, incident response, recovery, and improvement.

Why Attend this Course: Wins & Losses!

- Improve the ability to identify and manage cybersecurity risks.
- Strengthen readiness for security incidents.
- Build structured incident response plans.
- Reduce operational disruption during cyber incidents.
- Improve coordination between technical and business teams.
- Support faster containment and recovery.
- Improve documentation and evidence collection.
- Strengthen compliance and audit readiness.
- Identify gaps in cybersecurity controls.
- Support better communication during incidents.
- Improve cyber resilience through lessons learned.
- Build a practical approach for continuous risk improvement.

Conclusion

The Cybersecurity Risk Management and Incident Response course provides a practical framework for identifying, assessing, and managing cybersecurity risks while preparing organizations to respond effectively to security incidents. It covers the main stages of cyber risk and incident management, starting with understanding threats and business impacts, then assessing risks, planning controls, preparing response plans, handling incidents, and improving resilience.

The course follows a connected sequence that helps participants understand how cyber risk management and incident response work together. Risk assessment supports better control planning, while incident response ensures that the organization can act quickly when threats become real events.

By the end of the course, participants will have a practical understanding of how to manage cybersecurity risks, prepare response plans, coordinate incident actions, document evidence, recover services, and improve future readiness. The course supports stronger protection, clearer response responsibilities, reduced disruption, and improved cybersecurity resilience across the organization.

