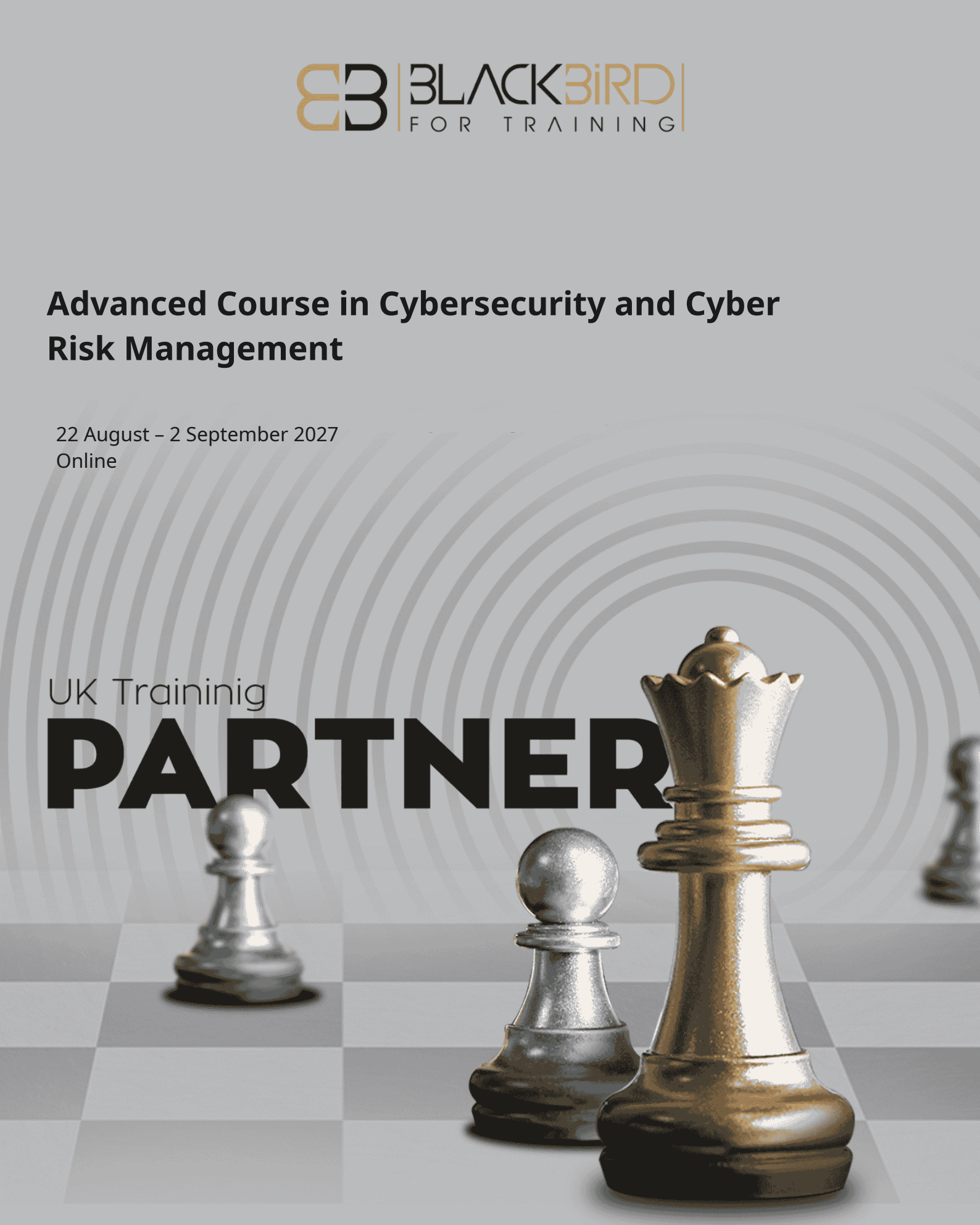
BLACKBIRD FOR TRAINING

Advanced Course in Cybersecurity and Cyber Risk Management

22 August – 2 September 2027
Online



Advanced Course in Cybersecurity and Cyber Risk Management

Ref: 3255029_329729 **Date:** 22 August – 2 September 2027 **Location:** Online **Fees:** 4900 GBP

Introduction

In light of the rapid digital transformations and significant technological advancements, cybersecurity threats have become a real challenge faced by organizations of all sizes and across various sectors. Cybersecurity is no longer just a technical option; it has become an essential component of organizational strategies to protect sensitive information and data, and to ensure business continuity.
This comprehensive training course aims to equip participants with both basic and advanced knowledge and skills in the field of cyber defense, with a strong focus on risk management methodologies and modern threat analysis. The course combines theoretical and practical aspects through real-world scenario simulations and hands-on applications, enabling participants to effectively develop their capabilities and build a more secure and stable work environment.

Course Objectives

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

- Build and lead an integrated cybersecurity strategy within their organization.
- Assess cybersecurity risks and prioritize mitigation actions.
- Implement effective security controls based on international best practices.
- Gain practical skills through real-world scenarios and simulations.

Course Outline

Day 1: Introduction to Cybersecurity and Risks

• Introduction to cybersecurity and its importance in the modern environment.
• The relationship between cybersecurity and enterprise risk management.
• Overview of modern cybersecurity threats.
• Introduction to the cybersecurity risk management lifecycle.

Day 2: Classification and Analysis of Cyber Threats

• Types of cyber threats and attacks.
• Analysis of internal and external threats.
• Case studies of major attacks on global organizations.
• Impact analysis.



Day 3: Vulnerability Assessment and Risk Evaluation

- Techniques for vulnerability detection.
- Identifying critical assets within the organization.
- Risk analysis tools Risk Matrix - Likelihood vs. Impact.
- Practical study: assessing risks in a technical project.

Day 4: Building Security Policies and Procedures

- How to develop effective information security policies.
- The role of policies in risk mitigation.
- Preparing standard operating procedures SOPs.
- Linking security policies to risk strategy.

Day 5: Network and Infrastructure Security

- Principles of secure network design.
- Network access management and control.
- Network segmentation and firewall implementation.
- Integration of intrusion detection and prevention systems IDS/IPS.

Day 6: Data Security, Encryption, and Access Management

- Data protection during transmission and storage.
- Encryption techniques and their types.
- Access management and privilege definition.
- Multi-factor authentication MFA and identity management.

Day 7: Cyber Incident Management and Response

- Methodology for incident handling.
- Steps for investigation and analysis.
- Incident logging and reporting.
- Developing an incident response plan.

Day 8: Business Continuity and Disaster Recovery

- Developing a business continuity plan BCP.
- Preparing a disaster recovery plan DRP.
- Integrating cybersecurity into emergency plans.
- Practical simulation exercise for crisis response.



Day 9: Strategic Cyber Risk Management

• Integrating risk management into corporate governance.
• Standards and frameworks e.g., ISO 27005 / NIST RMF.
• The role of senior leadership in supporting cybersecurity strategy.
• Periodic risk reviews and policy updates.

Day 10: Comprehensive Review and Practical Application

• Comprehensive hands-on application Cybersecurity Simulation Lab.
• Analyzing a real case and building a comprehensive cybersecurity plan.
• Team project presentations and discussion of evaluation results.
• Closing and certificate distribution.

Why Attend this Course: Wins!

• Strong focus on practical application through simulation labs and real case studies.
• Development of advanced risk analysis skills and formulation of preventive strategies.
• Empowering participants to effectively handle and respond to cybersecurity incidents.
• Preparing participants to comply with international cybersecurity standards and policies.
• Enhancing leadership and strategic planning capabilities within technical teams and organizations.

Conclusion

At the end of this course, participants will have acquired comprehensive expertise that qualifies them to face various cybersecurity challenges with confidence and efficiency. The skills gained will enable them to build effective protection strategies and develop a secure and stable environment within their organizations. Additionally, this course contributes to raising security awareness and promoting a cybersecurity culture among individuals and technical teams, making organizations more prepared to face future threats and protect their digital assets.

