BLACKBIRD FOR TRAINING

Cyber Security Policy & Management

10 – 14 May 2027
Kuala Lumpur (Malaysia)

UK Traininig
PARTNER



www.blackbird-training.com

Cyber Security Policy & Management

Ref: 3254306_165047 **Date:** 10 – 14 May 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

Welcome to the Advanced Cyber Security Policy & Management Course! This intensive program explores the most modern and cutting-edge concepts, strategies, and best practices in cyber security policy and management. Designed for professionals seeking to enhance their expertise, this course provides a comprehensive understanding of the challenges and opportunities in the rapidly evolving field of cybersecurity policy management.

Course Objectives

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

- Gain a deep understanding of cyber security policy frameworks and their application in modern organizations.
- Explore advanced techniques for managing cyber security risks, addressing threats, and mitigating vulnerabilities.
- Develop skills to create and implement effective cybersecurity strategies and policies.
- Understand the legal, ethical, and regulatory aspects of cyber security policies.
- Learn to communicate and collaborate effectively with stakeholders to enhance cybersecurity awareness and ensure compliance.
- Discover emerging trends and technologies in cyber security policy management.

Course Outlines

Day 1: Introduction to Cyber Security Policy & Management

- Comprehensive overview of cyber security policy and its importance in modern organizations.
- Understanding the current threat landscape and the evolving nature of cyber attacks.
- Introduction to major cyber security frameworks and standards, such as NIST and ISO 27001, and their role in protecting information assets.



Day 2: Risk Management and Assessment

- Core principles of cyber security risk management.
- Conducting cybersecurity risk assessments and vulnerability analyses to identify potential threats.
- Developing risk mitigation strategies and effective control mechanisms.
- Planning and managing incident response to minimize the impact of security breaches.

Day 3: Developing Cyber Security Policies and Procedures

- Formulating cyber security policies, standards, and guidelines to protect systems and information.
- Implementing access control and authentication mechanisms to secure sensitive data.
- Building security awareness and training programs to meet cyber security requirements.
- Planning for business continuity and disaster recovery to maintain secure operations.

Day 4: Legal and Regulatory Considerations

- Understanding the legal and regulatory frameworks related to cyber security policies and their impact on organizations.
- Overview of privacy and data protection laws, and their role in safeguarding customer information.
- Intellectual property considerations and their importance in cybersecurity policy.
- Compliance and cyber security audit requirements to ensure adherence to standards and avoid potential violations.

Day 5: Emerging Trends and Future Directions

- Exploring emerging technologies in cybersecurity, such as AI and blockchain, and their role in enhancing defenses.
- Cybersecurity governance and organizational structure to promote sustainable security practices.
- Strategic planning and leadership in cybersecurity to ensure effective protection across all organizational levels.
- Ethical considerations in cyber security and the importance of maintaining integrity in all practices.



Why Attend this Course: Wins & Losses!

- Gain a comprehensive understanding of what is cyber security policy and its significance in modern organizations.
- Learn to manage and implement cyber security policies effectively to protect your organization's digital assets.
- Prepare for roles such as cyber security policy analyst, cybersecurity specialist, and other leadership positions in cybersecurity management.
- Earn an Advanced Cyber Security Policy Certification, one of the best cyber security certifications to advance your career.
- Understand national and international cyber security policy frameworks, including national cyber security policies.
- Learn how to conduct cyber security assessments and manage cyber security audits to ensure compliance.
- Discover cyber security solutions that address current and emerging threats.
- Stay updated on emerging trends and technologies in cyber security policy management.

Conclusion

Upon completing the Advanced Cyber Security Policy & Management Course, participants will gain practical, advanced knowledge of cyber security policy management and the ability to address complex regulatory and technical challenges. With an Advanced Cyber Security Policy Certificate, participants will be well-prepared for roles such as cyber security policy analyst, cybersecurity specialist, or even leadership positions in cybersecurity management.

Join us to become a leader in the dynamic field of cyber security and secure your future in one of the world's fastest-growing industries!

