BLACKBIRD FOR TRAINING

Information Security & Cyber Security Workshop

4 – 8 October 2027
Kuala Lumpur (Malaysia)



Information Security & Cyber Security Workshop

Ref: 3254387_308847 **Date:** 4 – 8 October 2027 **Location:** Kuala Lumpur (Malaysia) **Fees:** 4900 GBP

Introduction

In today's digital era, where cyber threats are escalating in sophistication and frequency, information security management has become a vital aspect of organizational success. This workshop is designed to provide participants with the tools and knowledge to protect organizational assets, data, and systems from cyber risks. Through practical applications and theoretical insights, attendees will gain a solid understanding of what information security is, explore its definition and importance, and learn the fundamentals of cyber information security.

This information security training covers key concepts such as information security policies, risk mitigation techniques, incident response, and hands-on implementation of tools to enhance information technology security. By the end of the workshop, participants will be equipped to design, implement, and manage robust information security programs that align with industry standards and compliance requirements.

Workshop Objectives

By the end of this workshop, participants will:

- Understand why information security is important and its role in safeguarding organizational data.
- Learn the core concepts of information security management and how to implement them effectively.
- Gain insights into the responsibilities of an information security analyst and strategies for identifying vulnerabilities.
- Develop an actionable information security plan to mitigate cyber threats and vulnerabilities.
- Explore tools and frameworks for conducting information security audits and ensuring compliance.
- Examine information security policies that protect organizations from external and internal threats.
- Learn to integrate physical and IT security controls for a comprehensive information security program.
- Stay updated on cybersecurity trends, emerging threats, and modern information security services.



Workshop Outlines

Day 1: Cybersecurity Awareness

- What is information security? Definition, principles, and importance in modern organizations.
- Core principles: Confidentiality, integrity, and availability.
- Overview of cyber information security threats and their organizational impacts.
- Security baselining and addressing human-related security concerns.
- Practical session: Network discovery and identifying vulnerabilities through scanning and footprinting.

Day 2: Security Architecture

- Introduction to information technology security architecture and its importance.
- Exploring network segmentation, address translation, and access control mechanisms.
- The role of cryptography, permissions, and steganography in securing data.
- Hands-on training: Building a secure network architecture for enhanced protection.

Day 3: Identity Management & Network Hardening

- Fundamentals of identity management and its role in information security programs.
- Exploring authentication mechanisms, password policies, and federated identity systems.
- Techniques for network hardening, including securing administrative access and device protection.
- Best practices for traffic filtering and securing network devices.

Day 4: Software Security & Physical Security

- Identifying and mitigating software vulnerabilities through secure coding practices.
- The role of environmental monitoring and logging in vulnerability detection.
- Comprehensive overview of physical security controls and their integration with IT systems.
- Reviewing information security policies to ensure protection of human resources and devices.

Day 5: Incident Response & Cybersecurity Trends

- Developing an effective information security plan and incident response strategy.
- Understanding business continuity and disaster recovery planning.
- Insights into emerging cybersecurity trends, information security certification frameworks, and standards.
- The importance of continuous information security training to mitigate new threats.



Why Attend This Workshop: Wins & Losses!

- Comprehensive understanding: Gain in-depth knowledge of what information security is and how to implement it effectively.
- Practical application: Learn to design an actionable information security plan and conduct information security audits.
- Updated skills: Stay ahead of evolving threats through information security training and exposure to modern tools.
- Industry certification: Prepare for information security certification to enhance your professional credentials.
- Leadership in security: Develop the skills to lead information security programs that align with industry best practices.

Conclusion

This Cybersecurity and Information Security Management Workshop equips participants with the skills and knowledge to build resilient systems that protect organizations from evolving cyber threats. By mastering information security management, conducting thorough information security audits, and implementing robust information security policies, participants will be prepared to address real-world cybersecurity challenges with confidence.

Whether you are an information security analyst, a professional seeking information security certification, or a leader aiming to implement an effective information security program, this workshop provides a comprehensive pathway to success. Gain the skills, tools, and frameworks necessary to protect your organization and advance your career in the ever-critical field of cybersecurity.

