BLACKBIRD FOR TRAINING

Information Security & Cyber Security

25 – 29 April 2027
Online



Information Security & Cyber Security

Ref: 321492_294509 **Date:** 25 – 29 April 2027 **Location:** Online **Fees:** 2700 GBP

Introduction

In today's digital landscape, understanding information security is essential to safeguarding organizations from the growing range of cyber-attacks. This course provides participants with a comprehensive understanding of the key threats facing organizations and introduces essential information security techniques and controls to mitigate risks. Through detailed instruction, you will explore the basics of cybersecurity, how to design secure systems, and gain a global perspective on the various roles involved in providing a cohesive security solution.

In addition, you will review the latest trends in cyber threats, delve into information security best practices, and gain practical experience in managing security risks within an organization. By the end of the course, participants will have a clear understanding of how to implement information security strategies that align with organizational goals.

Course Objectives

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

- Understand cyber threats and vulnerabilities that organizations face and how to protect against them.
- Gain knowledge of information security basics, including techniques and controls to secure organizational systems.
- Learn the key components of an Information Security Management System ISMS.
- Explore various data protection principles and how to safeguard sensitive information.
- Identify and mitigate the impact of social engineering attacks, including common methods and techniques.
- Examine software vulnerabilities and understand security solutions to reduce the risk of exploitation.
- Understand physical security controls and the importance of integrating them with IT security.
- Explore the principles of information security and understand their application within an organization.
- Learn how cybersecurity protection and information security practices differ and complement each other.



Course Outlines

Day 1: Cybersecurity Awareness

- What is security? - Understanding the core concepts of security and its role in organizational protection.
- Confidentiality, integrity, and availability - Key principles of information security.
- Security baselining - Establishing a baseline for assessing security controls.
- Types of threats - A deep dive into the most common and emerging cyber threats.
- Security controls - Different levels of controls that can be implemented to prevent attacks.
- What is hacking? - Introduction to hacking techniques and how to defend against them.
- Risk management - Understanding how to assess and manage risks effectively.
- Data in motion vs. data at rest - Techniques for protecting data throughout its lifecycle.
- Network discovery - Tools and methods for discovering and securing network assets.

Day 2: Security Architecture

- Security architecture - Key components in designing a secure IT environment.
- Network devices and zones - Understanding how devices are configured to secure the network.
- Network segmentation and access control - Techniques for reducing attack surfaces and controlling access.
- Data security and cryptography - Implementing encryption and cryptographic protocols to protect sensitive data.
- Principles of permissions - Managing access to ensure the integrity of critical data and systems.

Day 3: Identity Management and Network Hardening

- What is identity management? - The role of identity and access management IAM in protecting digital assets.
- Authentication and directory services - Best practices for ensuring secure authentication processes.
- Cracking passwords - Techniques for testing password security and best practices for creating strong passwords.
- Federated identities and identity as a service IDaaS - Advanced methods for securing user identities across platforms.
- Network hardening - Securing network devices and limiting access to minimize vulnerabilities.
- Traffic filtering and remote access - Preventing unauthorized access to your network.



Day 4: Software Security and Physical Security

- Software engineering and security guidelines - How to incorporate security into the software development lifecycle.
- Software vulnerabilities - Analyzing common security weaknesses in software.
- Environment monitoring - Tools and techniques for actively monitoring for security events.
- Physical security controls - The intersection of physical security and information protection.
- Defense in depth - Multi-layered security strategies for maximizing protection.

Day 5: Incident Response and Cybersecurity Trends

- Types of disasters and incident investigation - Preparing for and responding to security incidents.
- Business continuity planning - Creating effective disaster recovery plans.
- Forensic incident response - Techniques for investigating and resolving security incidents.
- Cybersecurity trends - Emerging challenges and innovations in the cybersecurity space.
- Cybersecurity standards and training - Understanding the latest standards and best practices for ongoing staff education.

Why Attend this Course: Wins & Losses!

- Comprehensive Knowledge of Cybersecurity: By attending this course, you'll gain a solid understanding of the cybersecurity vs. information security debate, and know the essential components to secure any organization.
- Practical Skills: You'll gain hands-on experience with information security controls, helping you develop the practical skills needed to secure systems and mitigate risks.
- Career Growth: This course is an excellent starting point if you are looking to get into cybersecurity or become an information security analyst. It provides a foundational understanding of the information security analyst role, helping you step into a highly sought-after career.
- Real-world Application: Learn real-world information security best practices and strategies to implement in your organization immediately.
- Global Perspective: Understand how cybersecurity issues are handled worldwide, preparing you to deal with global challenges in cyber protection of an organization.

Conclusion

This course is designed to provide you with the essential tools and knowledge to protect your organization from cyber threats and understand the broader world of information security. Whether you are just beginning your journey into cybersecurity or looking to strengthen your existing knowledge, this course will equip you with the key principles and information security training needed to be successful. It will also open the door to career opportunities in the rapidly growing field of cybersecurity, where the demand for skilled information security analysts is at an all-time high.

