QUEST
Professional Center

PROFESSIONAL TRAINING COURSE

Course No. 1945

Cybersecurity Fundamentals & Information Security Management Training Course

CYBERSECURITY & INFORMATION SECURITY
INFORMATION TECHNOLOGY & CYBERSECURITY

DURATION
5 Days

DELIVERY
Classroom

Course Overview

The Cybersecurity Fundamentals & Information Security Management Training Course provides a comprehensive foundation in cybersecurity principles, information security management, organizational security governance, and practical protection measures. The course is designed to help professionals understand the cybersecurity landscape and develop the knowledge required to protect organizational information, systems, networks, applications, and digital services.

Participants will explore the core principles of information security, including confidentiality, integrity, and availability, together with common cyber threats, attack vectors, vulnerabilities, security controls, identity and access management, data protection, network security, endpoint security, and security monitoring.

The course also introduces the management dimension of information security, covering cybersecurity governance, security policies, risk assessment, security responsibilities, incident management, business continuity, security awareness, compliance, and performance measurement. Participants will learn how technical and organizational controls work together to reduce cybersecurity risk and support business objectives.

Through practical exercises, threat scenarios, risk assessment activities, security control reviews, incident-response simulations, and policy-development workshops, participants will develop a practical understanding of how to establish effective information security practices and contribute to a stronger organizational cybersecurity posture.

Objectives

- By the end of the course, participants will be able to:
- Explain fundamental cybersecurity and information security concepts.
- Analyze common cybersecurity threats, vulnerabilities, and attack techniques.
- Apply the principles of confidentiality, integrity, and availability.
- Identify critical information assets and technology resources.
- Assess basic cybersecurity risks and organizational exposure.
- Apply fundamental security controls to protect information and systems.

- Strengthen identity, authentication, and access management practices.
- Apply appropriate data protection and information security measures.
- Understand network, endpoint, application, and cloud security fundamentals.
- Develop and implement basic information security policies and procedures.
- Understand cybersecurity incident management and response processes.
- Support business continuity and information security resilience.
- Promote security awareness and responsible cybersecurity behavior.
- Understand cybersecurity governance, compliance, and accountability.
- Develop a practical foundation for continuous cybersecurity improvement.

Who Should Attend

This course is designed for IT professionals, cybersecurity professionals, information security specialists, system administrators, network administrators, technology support teams, and professionals who are responsible for protecting organizational information and technology resources.

It is also suitable for managers, supervisors, risk and compliance professionals, internal auditors, business continuity specialists, governance professionals, and employees who require a practical understanding of cybersecurity and information security management.

The course is particularly valuable for organizations seeking to establish a common cybersecurity knowledge foundation across technical and non-technical teams, strengthen security awareness, improve basic security controls, and develop stronger information security management practices.

Learning Outcomes

- By the end of the course, participants will be able to:
- Explain the fundamental concepts and objectives of cybersecurity.
- Describe the core principles of information security.
- Identify common cyber threats and attack methods.
- Recognize vulnerabilities and common security weaknesses.

- Identify critical organizational information assets.
- Perform basic cybersecurity risk identification and assessment.
- Apply fundamental security controls and protection measures.
- Explain identity, authentication, authorization, and access-control principles.
- Apply basic data, network, endpoint, and application security practices.
- Understand the fundamentals of cloud and remote-access security.
- Develop basic information security policies and procedures.
- Recognize cybersecurity incidents and support appropriate response activities.
- Understand business continuity and disaster recovery considerations.
- Support security awareness and cybersecurity culture initiatives.
- Understand cybersecurity governance, compliance, and accountability.
- Contribute to continuous improvement of organizational cybersecurity.

Course Outline

DAY 01

Cybersecurity and Information Security Fundamentals

- Understanding cybersecurity and information security.
- The role of cybersecurity in modern organizations.
- Confidentiality, integrity, and availability.
- Information assets and technology resources.
- Cybersecurity threats and threat actors.
- Common attack vectors and attack techniques.
- Malware, ransomware, phishing, and social engineering.
- Credential theft and identity-based attacks.
- Insider threats and human-related security risks.
- Understanding vulnerabilities and security weaknesses.
- Cybersecurity principles and organizational responsibilities.

DAY 01 — CONTINUED

PRACTICAL APPLICATION

Identify critical information assets, common threats, vulnerabilities, and potential security impacts within a representative organization.

DAY 02

Security Controls, Identity, Data, and Technology Protection

- Understanding cybersecurity controls.
- Preventive, detective, corrective, and compensating controls.
- Identity and access management fundamentals.
- Authentication and authorization.
- Password security and multi-factor authentication.
- Least privilege and access governance.
- Information classification and data protection.
- Encryption and secure information handling.
- Network security fundamentals.
- Endpoint and device security.
- Application security fundamentals.
- Cloud and remote-access security.

PRACTICAL APPLICATION

Assess a simulated organization's basic security controls and identify opportunities to strengthen identity, data, network, endpoint, and application protection.

DAY 03

Cybersecurity Risk Management and Information Security Policies

- Fundamentals of cybersecurity risk management.
- Identifying assets, threats, vulnerabilities, and risks.
- Risk likelihood and business impact.

DAY 03 — CONTINUED

- Basic risk assessment methodologies.
- Risk treatment and mitigation.
- Security policies, standards, procedures, and guidelines.
- Acceptable-use and information security policies.
- Access control and password policies.
- Data protection and information classification policies.
- Vulnerability and patch management policies.
- Security awareness requirements.
- Roles, responsibilities, and accountability.

PRACTICAL APPLICATION

Conduct a basic cybersecurity risk assessment and develop a set of information security policies and control requirements for a representative organization.

DAY 04

Incident Management, Monitoring, and Organizational Resilience

- Understanding cybersecurity incidents.
- Common types of security incidents.
- Incident detection and identification.
- Incident reporting and escalation.
- Incident response lifecycle.
- Containment, eradication, and recovery concepts.
- Security monitoring and logging fundamentals.
- Recognizing suspicious activities and indicators.
- Business continuity and disaster recovery.
- Information security during operational disruption.
- Third-party and supply-chain security considerations.
- Security awareness and human factors.

DAY 04 — CONTINUED

PRACTICAL APPLICATION

Participate in a simulated cybersecurity incident, identify the incident, assess its impact, establish response priorities, and develop recovery actions.

DAY 05

Information Security Management, Governance, and Continuous Improvement

- Information security governance fundamentals.
- Management responsibilities and security accountability.
- Cybersecurity compliance and regulatory considerations.
- Information security management systems.
- Security objectives and performance measurement.
- Cybersecurity metrics and reporting.
- Internal security reviews and control assessments.
- Identifying security gaps and corrective actions.
- Cybersecurity awareness and organizational culture.
- Continuous monitoring and improvement.
- Aligning information security with business objectives.
- Building a sustainable cybersecurity improvement program.

FINAL WORKSHOP

Develop an integrated Cybersecurity Fundamentals & Information Security Management framework covering information assets, threats, vulnerabilities, risk assessment, security controls, identity and access, data protection, policies, incident management, resilience, governance, awareness, performance measurement, and continuous improvement.

QUEST
Professional Center

Register or Request More Information

Course page: https://quest-training.com/courses/cybersecurity-fundamentals-information-security-management-training-course
Website: https://quest-training.com
Email: info@quest-training.com
Phone: +905016771440