CYBER SECURITY MANAGEMENT ITM014

COURSE DESCRIPTION

In today's digital-driven work environment, effective cybersecurity management is essential for safeguarding an organization's sensitive data, financial resources, and operational integrity. With the increasing sophistication of cyber threats, from phishing attacks to ransomware, businesses of all sizes face potential risks that can result in significant financial loss, reputational damage, and regulatory penalties. By implementing robust cybersecurity management, organizations can not only mitigate these risks but also foster a culture of security awareness, ensuring employees are vigilant and prepared to defend against cyber incidents.

The Cyber Security Management Course offers participants an in-depth exploration of the ever-evolving cybersecurity landscape and its inherent challenges. Designed to provide practical and theoretical knowledge, this course equips learners with the tools to protect digital assets, manage security operations, and respond to cyber threats effectively. From understanding fundamental cybersecurity concepts to mastering advanced incident response techniques, participants will gain critical insights into the mechanics of cyberattacks, security governance, and regulatory frameworks.

COURSE GOAL

To enhance participants' knowledge, skills, and abilities necessary to be fully prepared to lead cybersecurity initiatives and make informed decisions in safeguarding organizational infrastructure

COURSE OBJECTIVES

By the end of this course, participant will have:

- Covered the various areas of Cyber Security
- Obtained notions of user safety - individual behavior (passwords, email, mobility, social networks) and basic notions of Cyber Security
- Obtained answers to the following questions:
  - What is the purpose of Cybersecurity?
  - How to manage security?
  - What are the security and defense controls?
  - What are the means to respond to security incidents?
- Understood how an attack is performed
- Reviewed the context of regulation
- Reviewed ethics and standards related to Cyber Security

WHO SHOULD ATTEND

This course is ideal for:

- IT and Security Professionals: Individuals responsible for managing or securing digital infrastructure, including security analysts and network administrators.
- Executives and Management Levels: Leaders overseeing cybersecurity strategies, policies, and decision-making within organizations.
- Risk Managers and Officers: Professionals tasked with identifying, assessing, and mitigating cyber risks.
- Compliance Managers and Officers: Those ensuring organizational adherence to cybersecurity regulations and standards.
- Auditors: Individuals involved in auditing security measures and ensuring their effectiveness.

It is designed for anyone looking to strengthen their understanding of cybersecurity management and its critical role in protecting organizational assets.

COURSE DURATION

5 Working Days

COURSE OUTLINES

1. Threats and Attacks
    - What are the threats?
    - Understand how an attack occurs
    - Attacker profiles
2. Information Security Basics
    - What is the purpose of Cyber Security?
    - Basics: Basic triad, notions of risk, threat, vulnerability, impact
    - The return on investment of security
    - Security lines of defense
3. Information Security Management and Governance
    - How to manage security
    - Roles and responsibilities
    - Security controls
    - Security policies

4. Audits and Tests
    - Security audits
    - Security testing
    - Pen tests
5. Security Incident Management
    - How to manage security incidents
    - Security Operation Center (SOC) -Computer Security Incident Response Team (CSIRT)
    - Crisis management
6. Software security
    - Software development and application security
    - Software security testings, xAST
    - DevOpsSec
7. Cloud and Mobile Security
    - Cloud security controls – CASB
    - Mobile device security
8. Security Awareness
    - User security concepts -individual behavior
    - Methods