FORTIFYING DIGITAL DEFENSES THROUGH CYBERSECURITY AND ISO STANDARDS

Certificate in Cybersecurity Awareness and ISO 27001

Course Code: M019/25

Duration: 16 Hours

Delivery Format: Hybrid

Target Audience:

- IT professionals seeking to enhance their cybersecurity knowledge.
- Business executives and managers responsible for overseeing organizational security.
- Employees at all levels who handle sensitive information.
- Anyone interested in understanding ISO 27001 and its implications for information security.

Program Outcomes:

Upon completion of this program, participants will be able to:

- Understand fundamental cybersecurity principles and their importance in protecting digital assets.
- Comprehend the key concepts and requirements of relevant ISO standards for cybersecurity.
- Identify cybersecurity threats and vulnerabilities and implement appropriate safeguards.
- Develop and implement cybersecurity policies and procedures within an organization.
- Enhance an organization's overall cybersecurity posture and resilience.

Detailed Syllabus

Module 1: Introduction to Cybersecurity Awareness

Outcome: Participants will be able to understand fundamental cybersecurity concepts, common threats, and basic best practices. They will also recognize the role of human error in cyber attacks.

Topics:

- Understanding Cybersecurity and its importance
- Common Threats and Risks in Cybersecurity
- Basic Cybersecurity Best Practices
- Understanding the Role of Human Error in Cyber Attacks

Activities:

- Interactive lectures and discussions on cybersecurity principles.
- Case studies of real-world cyberattacks and their impact.

Assessments:

- Quiz on cybersecurity terminology and key concepts.
- Short answer questions on the importance of cybersecurity.

Module 2: Phishing Attacks

Outcome: Participants will be able to define phishing attacks, identify different types and techniques, and understand how to respond and implement security measures against them.

Topics:

- What are Phishing Attacks?
- Different Types of Phishing Attacks
- Techniques Used in Phishing
- Identifying Phishing Emails
- Understanding How to Respond to Phishing Emails
- Security Measures for Phishing Attacks

Activities:

- Detailed presentations on the nature and types of phishing attacks.
- Analysis of sample phishing emails to identify red flags.

Assessments:

- Practical exercise: Identifying phishing emails in a set of samples.
- Quiz on phishing techniques and prevention methods.

Module 3: Social Engineering Attacks

Outcome: Participants will be able to define social engineering attacks, recognize tactics, and implement defense strategies and response protocols.

Topics:

- What are Social Engineering Attacks? Definition, Tactics, and Real-World Attacks
- Techniques Used in Social Engineering Attacks
- Defending Against Social Engineering Attacks
- Understanding How to Respond to Social Engineering Attacks

Activities:

- Lectures on social engineering definitions, tactics, and real-world examples.
- Case study analysis of significant social engineering breaches.

Assessments:

- Case study analysis: Developing a mitigation plan for a social engineering attack.
- Quiz on social engineering techniques and countermeasures.

Module 4: ISO 27001 Awareness

Outcome: Participants will be able to understand the ISO 27001 standard's purpose, benefits, clauses, controls, and implementation process.

Topics:

- Understanding the ISO 27001 Standard - Its Purpose, Benefits, Clauses, and Controls
- Overview of Implementing ISO 27001
- ISO 27001 Implementation Process

Activities:

- Detailed presentations on the ISO 27001 standard.
- Explanation of the standard's clauses and controls.

Assessments:

- Quiz on ISO 27001 terminology and core concepts.
- Short answer questions on the importance of ISO 27001.

Module 5: Data Protection and Privacy

Outcome: Participants will be able to understand data protection and privacy principles, key regulations, types of data breaches, and methods for implementing data security.

Topics:

- Understanding Data Protection and Privacy
- Key Principles and Regulations on Data Protection
- Different Types of Data Breaches
- Implementing Data Security and Sensitive Data Handling

Activities:

- Lectures on data protection and privacy concepts and regulations.
- Case studies of various types of data breaches.

Assessments:

- Quiz on data protection principles and regulations.
- Short essay on the importance of data privacy.

Module 6: Network Security and Cyber Attacks

Outcome: Participants will be able to understand network security fundamentals, types of network-targeting cyber attacks, and best practices for securing networks and responding to attacks.

Topics:

- Understanding Network Security
- Types of Cyber Attacks Targeting Networks
- Best Practices for Securing Networks
- Identifying and Responding to Cyber Attacks

Activities:

- Presentations on network security concepts and cyber attack types.
- Demonstrations of common network attacks.

Assessments:

- Quiz on network security terminology and attack types.
- Short answer questions on network security best practices.