Module 1: Introduction to Cyber security & Risk Management

Course Outline

1. Fundamentals of Cyber security

- Definition and scope of cyber security
- Importance of data protection and privacy
- Types of cyber threats (malware, phishing, ransom ware, etc.)

2. Information Security Principles

- CIA Triad (Confidentiality, Integrity, Availability)
- Security policies and procedures
- Role of encryption and authentication

3. Risk Assessment and Management

- Identifying and classifying risks
- Risk mitigation and control strategies
- Building an enterprise risk management framework

4. Cyber security Governance and Compliance

- Introduction to international security standards (ISO 27001, NIST)
- Legal and ethical aspects of cyber security

- Organizational responsibilities and best practices

5. Incident Response Planning

- Developing and implementing incident response plans
- Detecting, responding to, and recovering from cyber incidents
- Post-incident analysis and continuous improvement

Learning Outcomes

- By the end of this module, learners will be able to:
- Understand the fundamental principles of cyber security and information assurance.
- Identify and analyze potential cyber risks within an organization.
- Apply appropriate risk mitigation and governance strategies.