Security Controls Fundamentals

Duration: 1 day

- **Overview of Information Security Controls**
  - Purpose and Importance of Security Controls
  - Categories of Controls: Preventive, Detective, Corrective
  - Mapping Controls to Risk Management
- **Administrative (Managerial) Controls**
  - Security Policies and Standards
  - Security Awareness and Training
  - Background Checks and Job Rotation
  - Access Control Policies
- **Technical (Logical) Controls**
  - Authentication and Authorization
  - Encryption and Data Masking
  - Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS)
  - Endpoint Protection and Antivirus Tools
  - Network Access Controls and VPNs
- **Physical Controls**
  - Facility Access Controls (Badges, Biometrics)
  - Surveillance and Monitoring Tools
  - Environmental Controls (Power, Fire Suppression)
  - Physical Barriers and Locking Mechanisms
- **Control Implementation Considerations**
  - Selecting Appropriate Controls Based on Risk and Environment
  - Layered Security (Defense in Depth)
  - Principle of Least Privilege and Segregation of Duties
- **Control Validation and Maintenance**
  - Logging and Monitoring for Control Effectiveness
  - Regular Reviews and Audits
  - Updating Controls Based on New Threats
- **Standards and Frameworks Overview**
  - Control Mapping in ISO/IEC 27001
  - NIST Categories and Control Families (High-Level View)

- **Summary and Q&A**
    - Recap of Control Types and Their Functions
    - Open Discussion and Clarifications