Control Testing, Maturity & Gap Assessment

Duration : 24 Hours

This 24-hour program provides participants with a comprehensive understanding of control design, control effectiveness testing, maturity assessment methodologies, and gap remediation planning. Learners will gain hands-on knowledge of industry frameworks (ISO 27001, NIST, COBIT, CMMI, ISO 21827), evaluation techniques, scoring mechanisms, and reporting methods. The course equips professionals to perform control testing, conduct maturity assessments, identify gaps, prioritize remediation actions, and develop structured improvement roadmaps for security and compliance programs.

Prerequisites

Participants should ideally have:

- Basic understanding of information security concepts
- Familiarity with governance, risk, and compliance (GRC) terminology
- Exposure to ISO 27001, NIST CSF, or similar frameworks (recommended, not mandatory)
- Experience working in security operations, audit, risk management, or IT governance roles (preferred).

Day 1: Control Design & Assurance Frameworks

- Types of controls
  - Preventive
  - Detective
  - Corrective
- Control design vs operational effectiveness
  - Understanding design adequacy
  - Evaluating implementation and effectiveness
  - Common gaps observed in organizations
- Mapping controls across frameworks
  - ISO 27001
  - NIST

    - COBIT
- Audit evidence, sampling, and validation techniques
    - Types of evidence: documentary, technical, observational
    - Sampling techniques
        - Random
        - Judgmental
        - Statistical
    - Validation steps – inspection, re-performance, corroboration
- Documentation of test procedures and recording results

Day 2: Maturity Models & Evaluation Methodologies

- Overview of maturity models
    - CMMI
    - ISO 21827 (SSE-CMM)
- Control maturity levels – Initial to Optimized
- Evaluation criteria, scoring mechanisms, and ratings
    - Developing scoring rubrics
    - Weightage assignment for controls
    - Consistency and normalization in scoring
- Building maturity matrices for ISMS and TPRM programs
- Case Study: Assessing and scoring ISMS maturity for a sample supplier

Day 3: Gap Identification & Remediation Planning

- Conducting a control gap assessment
    - Approach
    - Templates
    - Workflows

Control Testing, Maturity & Gap Assessment

Duration : 24 Hours

- Analyzing findings and prioritizing remediation actions
    - Using impact-likelihood models
    - Risk-based prioritization
    - Resource and cost considerations
- Linking identified control deficiencies to a risk register
- Reporting and communicating results to management
    - Structure of a professional assessment report
    - Presenting severity, implications, and recommendations
    - Handling stakeholder questions and objections
- Practical Workshop: Developing a 30/60/90-day remediation roadmap