CONCEPT

Information Security Management Essentials: ISMS, Risk and Security Controls

Information Security Management Essentials: ISMS, Risk and Security Controls

Technical depth: Practitioner · **Practical mode:** Case study

Introduction

Many organisations invest in security tools yet still lack an inventory of what they protect, an agreed view of risk and a policy set that people actually follow. Breaches then expose gaps that no single product could close. This Core Concept course gives managers the working method to run information security as a managed programme, from asset inventory and risk assessment through policies, access control, incident handling and measurement. Participants test each method against case material from several sectors and leave with an Information Security Programme Plan for their own organisation.

Course Objectives

- Assess an organisation's current security posture using a NIST CSF 2.0 profile, an asset inventory and a requirements register
- Interpret ISO/IEC 27001:2022, ISO/IEC 27002:2022 and the CIS Controls v8.1 and select the elements that fit the organisation's context
- Conduct an information security risk assessment and choose treatment options in line with ISO/IEC 27005:2022
- Establish classification, policy and access management arrangements proportionate to the risks identified
- Organise incident, vulnerability, supplier and continuity controls and measure their performance with defined metrics
- Produce an Information Security Programme Plan that can be presented to management for approval

Target Audience

- Information security managers and ISMS coordinators running a security programme
- IT managers accountable for protecting systems, networks and data
- Risk and compliance managers responsible for information risk
- Data, records and document control managers overseeing classification and handling
- Operations and shared services managers who own critical information assets

Course Outline

Day 1: The Security Landscape and Current-State Assessment

- ISO/IEC 27000 Vocabulary: Confidentiality, Integrity and Availability
- Threat Landscape Analysis with MITRE ATT&CK Tactics
- Information Asset Inventory and Ownership Register
- Security Posture Baseline Using a NIST CSF 2.0 Current Profile
- Legal, Contractual and Regulatory Requirements Register

Day 2: Security Frameworks and Standards

- ISO/IEC 27001:2022 Clauses 4 to 10 and the Plan-Do-Check-Act Cycle
- ISO/IEC 27002:2022 Control Themes and Attributes
- NIST CSF 2.0 Functions: Govern, Identify, Protect, Detect, Respond and Recover
- CIS Controls v8.1 Implementation Groups and Safeguards
- Framework Crosswalk: ISO/IEC 27001, NIST CSF 2.0 and CIS Controls

Day 3: Running the Core Security Processes

- Information Security Risk Assessment and Treatment with ISO/IEC 27005:2022
- Information Classification Scheme and Handling Rules
- Information Security Policy Set: Top-Level and Topic-Specific Policies
- Access Management Procedure: Least Privilege, Joiners-Movers-Leavers and Access Reviews
- Security Awareness Programme Design and Phishing Simulation Metrics

Day 4: Incidents, Vulnerabilities and Measurement

- Incident Management Process under ISO/IEC 27035-1:2023
- Vulnerability and Patch Management with CVSS v4.0 Scoring
- Supplier Security Requirements and the Cloud Shared Responsibility Model
- Information Security Continuity Using an ISO 22301 Business Impact Analysis
- Security Metrics and KPI Design under ISO/IEC 27004

Day 5: Case Work and the Information Security Programme Plan

- Healthcare Ransomware Case Study: Tracing Control Failures
- Retail Data Leakage Case Study: Supplier Access Misuse
- Control Gap Analysis Against ISO/IEC 27002:2022 for an Own Organisation
- Information Security Programme Plan Drafting
- Peer Review Panel and Plan Defence

Skills You Will Gain

- Information Asset Management
- Security Risk Assessment
- Control Framework Mapping
- Security Policy Development
- Access Governance
- Security Incident Coordination
- Security Performance Measurement

Why Attend This Course

- Return to work with an Information Security Programme Plan built on your own assets, risks and gaps
- Explain security priorities to management in terms of risk and business impact rather than tools
- Recognise the control weaknesses behind common breaches before they occur in your own environment
- Compare practice with managers from other sectors and countries who face similar threats

Conclusion

Information security holds only when assets are known, risks are understood and controls are owned, tested and measured. This course moves from establishing the current security posture, through the principal international standards and frameworks, to the everyday processes and the incident, vulnerability and supplier issues that most often cause breaches. The final day turns this into an Information Security Programme Plan that participants take back to management, giving them a structured basis for directing security effort where it matters.