CONCEPT

ISO 27005 Information Security Risk Management: Assessment, Treatment and Acceptance

ISO 27005 Information Security Risk Management: Assessment, Treatment and Acceptance

Introduction:

Many organisations run an information security risk assessment once a year, yet the results rarely drive decisions: risk criteria are vague, likelihood scores are guesses, the register lists assets rather than scenarios and treatment choices are not traceable to controls. This Core Concept course examines ISO 27005 information security risk management in depth, from context and risk criteria through scenario analysis, evaluation, treatment, acceptance and review. Participants compare the ISO/IEC 27005 approach with other published methods and complete a full assessment on a case, producing an Information Security Risk Assessment Report and Risk Treatment Plan.

Course Objectives:

- Establish the context, scope and risk criteria for an information security risk assessment in line with ISO/IEC 27005:2022
- Select between event-based and asset-based identification and justify the choice for a given scope
- Analyse threats, vulnerabilities and consequences using calibrated likelihood and consequence scales
- Evaluate and prioritise risks in a register that records owners, scenarios and risk levels
- Decide risk treatment options, link them to ISO/IEC 27001 Annex A reference controls and document residual risk for acceptance
- Present assessment results to management and set monitoring and review triggers for reassessment

Target Audience:

- Managers who lead information security risk assessments across business units
- ISMS managers accountable for the risk assessment and treatment process
- Risk analysts who build and maintain information security risk registers
- Security architects who translate risk scenarios into control decisions
- IT and business risk owners who approve treatment plans and accept residual risk

Course Outline:

Day 1: Risk Management Context and Criteria

- ISO/IEC 27005:2022 Structure and Its Relationship to ISO 31000 and ISO/IEC 27001
- Internal and External Context Analysis for the Risk Assessment Scope
- Risk Acceptance Criteria and Criteria for Performing Assessments
- Risk Owner Identification and Accountability Matrix
- Maturity Review of an Existing Risk Assessment Methodology

Day 2: Identification Approaches and Alternative Methods

- Event-Based Identification: Risk Sources, Objectives and Strategic Scenarios
- Asset-Based Identification: Primary Assets, Supporting Assets and Their Dependencies
- OCTAVE Principles for Risk-Based Security Assessment
- EBIOS Risk Manager: Iterative Analysis from Missions to Technical Functions
- NIST SP 800-30 Rev. 1 Assessment Process and Three-Tier Hierarchy

Day 3: Threat, Vulnerability and Risk Analysis

- Threat Catalogue and Threat Source Characterisation
- Vulnerability Identification from Scan Results, Audit Findings and Incident Records
- Likelihood and Consequence Scales: Qualitative, Semi-Quantitative and Quantitative
- Risk Analysis Worksheet and Risk Level Matrix Calibration
- Risk Evaluation and the Prioritised Information Security Risk Register

Day 4: Treatment, Residual Risk and Review

- Treatment Option Selection: Avoid, Share, Mitigate or Accept
- Risk Treatment Plan Traceability to ISO/IEC 27001 Annex A Reference Controls
- Residual Risk Estimation and Formal Risk Acceptance Records
- Assessment Pitfalls: Scoring Bias, Double Counting and Aggregated Scenarios
- Monitoring and Review Triggers, Key Risk Indicators and Reassessment Cycles

Day 5: Full Risk Assessment Workshop on a Case

- Case Workshop: Context, Scope and Risk Criteria for a Payment Services Provider
- Case Workshop: Scenario Building and Likelihood and Consequence Scoring
- Case Workshop: Evaluation, Treatment Decisions and Residual Risk
- Information Security Risk Assessment Report and Risk Treatment Plan Drafting
- Management Risk Briefing and Risk Acceptance Challenge Panel

Skills You Will Gain:

- Risk Criteria Design
- Risk Scenario Construction
- Threat and Vulnerability Analysis
- Likelihood and Consequence Calibration
- Risk Register Management
- Treatment Option Appraisal
- Residual Risk Justification
- Risk Method Comparison

Why Attend This Course:

- Return with an Information Security Risk Assessment Report and Risk Treatment Plan built through a complete case assessment
- Replace inconsistent scores with scales and criteria that different assessors apply the same way
- Defend treatment and acceptance decisions to management with a clear line from scenario to control
- Compare assessment practice with risk specialists from finance, healthcare, government services and technology

Conclusion:

Information security risk assessment is useful only when criteria are agreed, scenarios are realistic, scores are consistent and treatment decisions can be traced and reviewed. This course moves from context and risk criteria, through event-based and asset-based identification and the alternative published methods, to threat, vulnerability and consequence analysis, treatment, residual risk and review. The final day applies the whole ISO/IEC 27005 process to a case and produces an Information Security Risk Assessment Report and Risk Treatment Plan ready for management review.