

ISO/IEC 27005 Specialist Training Course



TRECCERT ISO/IEC 27005 Specialist is an advanced-level course developed to provide trainees with a solid knowledge of the ISO/IEC 27005 guidelines and controls. The training course provides an in-depth explanation of guidelines and controls mandated to establish, implement, manage, improve and assess an Information Security Risk Management (ISRM).

TARGET AUDIENCE

The ISO/IEC 27005 Specialist training course is developed for professionals seeking to expand their professional skills on the assessment and management of an information security risk management process, for example:

- Information Security Risk Manager, Team Leader or Technician
- Business Owner, COO, CIO, CISO
- Risk Analyst, Model Risk Specialist, Risk Manager

LEARNING OBJECTIVES

- › Know and understand the purpose of an information security risk management process, including basic concepts, principles and other risk management frameworks.
- › Know and understand the whole information security risk management process steps and activities.
- › Know, understand and be able to identify, assess and treat the information security risks and perform other related activities.
- › Know and understand the basic analysis and methods used to establish a risk management context, assess and manage information security risks and implement security controls.
- › Know, understand and be able to support the information security risk manager perform risk management activities.

COURSE MATERIAL FACTSHEET



Training Slides
300



Quiz Questions
20



Exercises
2

COURSE OUTLINE

1. Information Security Risk Management

Information Security Background
Risk Management Background
Information Security Risk
Information Security Risk Management Process based on ISO 27005 Standard
Statement of Applicability and Risk Management
Risk Heat Maps

2. Establishing the Context of the Information Security Risk Management Process

Context Establishment
Information Security Risk Management Process Basic Criteria
Information Security Risk Management Scope and Boundaries
Defining the Organization's Structure

3. Information Security Risk Assessment

Information Security Risk Assessment Approaches
Identification of Information Security Risks
Information Security Risk Analysis
Evaluation of Information Security Risks

4. Information Security Risk Treatment

Risk Treatment Options and Techniques for Selecting such Options
Risk Treatment Plan Development and Residual Risk Evaluation
Acceptance of Information Security Risks
Risk Recording and Reporting

5. Risk Communication and Consultation

Overview of Risk Communication and Consultation
Risk Communication and Consultation Phases and Plan
Risk Communication and Consultation Techniques

6. Risk Monitoring and Review

Overview of the Risk Monitoring and Review Process
Monitoring, Reviewing and Improving the Information Security Risk Management Process

EXAMINATION DETAILS



Nr. of questions
100



Type of exam
Multiple choice



Duration
2 hours



Location
Online

COURSE DETAILS



Duration
Three (3) days



Language
English



Credits
24



Training mode
Classroom and online

PATH TO RECOGNITION

info@treccert.com | www.treccert.com

