

## Implementing Information Security with ISO/IEC 27002 Certification - 2 Days

### Preparing for the Security Foundation Certification Exam

*Course 2005 Overview*

- You Will Learn How To**
- Prepare for and take the EXIN Information Security Foundation (ISF) exam based on ISO/IEC 27002
  - Confidently explain and define an array of security terminologies
  - Navigate the complexities of threats and risks in your organization
  - Maintain a robust security infrastructure that responds effectively to security incidents
  - Deploy security countermeasures against a wide range of malware attacks
  - Ensure compliance with vital information technology laws and regulations
- Course Benefits** ISO/IEC 27000 is a globally-recognized set of standards that outlines best practices in information security for your organization. This course prepares you for the EXIN ISF Certification exam based on ISO/IEC 27002. You gain knowledge of standard security terminologies and practices needed to pass the examination.
- Who Should Attend** Anyone who wants a basic understanding of information security, from entry-level personnel to executive managers. This course is also valuable for those seeking a career in information technology as well as those whose organizations are preparing for the ISO/IEC 27002 certification.
- Workshop Course** Workshops and practice exam questions provide you with practical experience preparing for the EXIN ISF Certification exam based on the ISO/IEC 27002. Workshops include:
- Taking practice exams at the end of each chapter
  - Protecting communication with encryption and digital signatures
  - Detecting threats and vulnerabilities on your system
  - Analyzing a privacy incident case study and documenting solutions

## Implementing Information Security with ISO/IEC 27002 Certification - 2 Days

### Preparing for the Security Foundation Certification Exam

*Course 2005 Outline*

#### Introduction to ISO/IEC 27002 Security Foundation

- Examination and certification goals
- Blueprint of the Information Security Foundation exam
- Assessing your initial readiness

#### Defining Information and Data Security

##### Examining the importance of data

- Data and information systems
- Storing, communicating and processing information

##### What is information security?

- Protecting the security objectives: confidentiality, integrity and availability
- Determining the value of information

##### Assessing the CIA model

- Implementing confidentiality measures
- Ensuring integrity with accurate information
- Guaranteeing availability for continuity and timely operations
- Creating an information architecture

#### Analyzing Threats and Risks to the Organization

##### Evaluating threats to your organization

- Measuring how assets are at risk
- Detecting vulnerabilities that threaten operations

##### Performing risk analysis

- Evaluating the benefits of quantitative vs. qualitative risk analysis
- Deploying countermeasures to defeat threats and reduce risk

#### Managing a Balanced Approach to Information Security

##### Directing support for information security

- Defining a security policy and its purpose in your organization
- Examining the components of a security policy
- Achieving in-depth security with a multilevel defense

##### Documenting security objectives

- Managing the goals of internal security
- Maintaining sound external policy practices

- Assigning roles and responsibilities

##### Responding to security incidents

- Effectively communicating security events
- Documenting different events and weaknesses
- Establishing and following escalating procedures

#### Implementing Security Countermeasures

##### Enumerating types of security countermeasures

- Preventing intrusions and attacks
- Detecting security breaches
- Suppressing the damage of a security incident
- Applying corrective measures to restore integrity
- Transferring risk by insuring against loss

##### Controlling access to information

- Creating a classification scheme
- Labeling and handling information as an asset

##### Enhancing security with cryptography

- Managing access with encryption
- Guaranteeing authenticity with digital signatures
- Ensuring integrity with hashing

##### Assessing threats to your organization

- Detecting viruses and hoaxes
- Preventing SPAM and phishing fraud
- Countering logic bombs and Trojan horses
- Defending against the threat of spyware, worms and rootkits

##### Assessing Legal Requirements

##### Complying with legislation and regulations

- Upholding security standards and policies
- Verifying compliance

##### Adhering to legislative and regulatory measures

- Defending intellectual property rights
- Managing organizational records
- Safeguarding personal information
- Preventing misuse of information

#### Final Review and Preparation

- Priming for the exam
- Identifying the exam requirements
- Handling difficult questions
- Managing time and progress during the exam
- Assessing readiness