

Exam requirements

Information Security Foundation based on ISO/IEC 27002 (ISFS.EN)

Publication date	01-12-2009	
Start date	01-10-2008	
Summary	<p>Information security is becoming increasingly important. Globalization of the economy leads to a growing exchange of information between organizations (their employees, customers and suppliers) and a growing use of networks, such as the internal company network, connection with the networks of other companies and the Internet. Furthermore, activities of many companies now rely on ICT, and information has become a valuable asset. Protection of information is crucial for the continuity and proper functioning of the organization: information must be reliable.</p> <p>In the Information Security Foundation module, based on ISO/IEC 27002 (ISFS), the basic concepts of information security and their coherence are tested.</p>	
Target group	<p>The target group of ISFS is everyone in the organization. The basic knowledge that is tested in this module contributes to the understanding that information is vulnerable and that measures are necessary to protect this information. The module is also suitable for small independent businesses for whom some basic knowledge of information security is necessary.</p> <p>This module can be a good start for new information security professionals.</p>	
Context	<p>The Certificate Information Security Management Advanced based on ISO/IEC 27002 is a follow up of the Certificate Information Security Foundation based on ISO/IEC 27002.</p>	
Prerequisites	None.	
Practical assignment	Not applicable	
Examination details	Examination type:	Computer-based or paper-based multiple choice.
	Time allotted for examination:	60 minutes
	Number of multiple-choice questions:	40
	Pass mark:	65% (26 out of 40)

Open book: no
Electronic equipment permitted: no
Sample questions To prepare for your examination you can download the sample exam on the previous page for free.

Exam requirements	1. Information and security	10%
	2. Threats and risks	30%
	3. Approach and organization	10%
	4. Measures	40%
	5. Legislation and regulations	10%

Specification of the exam requirements

1. Information and security	1.1 The concept of information (2.5%)
	1.2 Value of information (2.5%)
	1.3 Reliability aspects (5%)
2. Threats and risks	2.1 Threat and risk (15%)
	2.2 Relationships between threats, risks and the reliability of information. (15%)
3. Approach and Organization	3.1 Security policy and security organization (2.5%)
	3.2 Components (2.5%)
	3.3 Incident Management (5%)
4. Measures	4.1 Importance of measures (10%)
	4.2 Physical security measures (10%)
	4.3 Technical measures (10%)
	4.4 Organizational measures (10%)
5. Legislation and regulations	5.1 Legislation and regulations (10%)

List of basic concepts

This part contains the terms with which candidates should be familiar. Terms are listed in order of Exam requirement. To avoid repetition, terms have usually been listed under the first examination specification where they are used. Note that questions based on one of the examination requirements may also use terms listed under the heading for other requirements.

- 1 Information and security
 - 1.1 The concept of information
 - Data
 - Informatics
 - Information
 - Information analysis
 - Information architecture

- Storage medium
- Information management
- Information system
- Infrastructure
- 1.2 Value of information
 - Asset
 - Production factor
- 1.3 Reliability aspects
 - Availability
 - Continuity
 - Robustness
 - Timeliness
 - Integrity
 - Authenticity
 - Verifiability
 - Correctness
 - Validity
 - Precision
 - Nonrepudiation
 - Completeness
 - Confidentiality
 - Exclusivity
 - Privacy
- 2 Threats and risks
 - 2.1 Threat and risk
 - Security measure
 - Preventive
 - Detective
 - Repressive
 - Corrective
 - Threat
 - Hacking
 - Vulnerability
 - Phishing
 - Risk
 - Risk assessment (Dependency & Vulnerability analysis)
 - Risk analysis
 - Qualitative risk analysis
 - Quantitative risk analysis
 - Risk management
 - Risk strategy
 - Risk bearing
 - Risk neutral
 - Risk avoiding
 - Damage
 - Direct damage
 - Indirect damage
 - Spam
 - Spyware

- Virus
 - Worm
- 3 Approach and Organization
- 3.1 Security policy and security organization
- Security Policy
 - Security Organization
 - Category
 - Impact
 - Priority
 - Urgency
- 3.2 Components
- Code of Conduct
- 3.3 Incident Management
- Security incident
 - Escalation
 - Functional escalation
 - Hierarchical escalation
 - Incident cycle
 - ISO/IEC 20000:2005
- 4 Measures
- 4.1 Importance of measures
- Classification (grading)
- 4.2 Physical measures
- Authentication
 - Biometrics
 - Clean desk policy
 - Interference
 - Uninterruptible Power Supply (UPS)
- 4.3 Technical measures
- Access control
 - Backup
 - Botnet
 - Certificate
 - Cryptography
 - Digital signature
 - Encryption
 - Hoax
 - Logical access management
 - Malware
 - Maintenance door
 - Patch
 - Personal firewall
 - Public Key Infrastructure (PKI)
 - Rootkit
 - Key
 - Social engineering
 - Trojan
 - Validation

- Virtual Private Network (VPN)
- 4.4 Organizational measures
- Authorization
 - Business Continuity Management (BCM)
 - Business Continuity Plan (BCP)
 - Disaster
 - Disaster Recovery Plan (DRP)
 - Segregation of duties
 - Identification
 - Stand-by arrangement
 - Change Management
- 5 Legislation and regulations
- 5.1 Legislation and regulations
- Public records legislation
 - Audit
 - Copyright legislation
 - Code of practice for information security (ISO/IEC 27002:2005)
 - Compliance
 - Security regulations for the government
 - Security regulations for special information for the government
 - Personal data protection legislation
 - Computer criminality legislation

Literature

- A. Hintzbergen, J., Baars, H., Hintzbergen, K. and Smulders, A.
The Basics of Information Security - A practical handbook*

Copyright © 2009 EXIN

All rights reserved. No part of this publication may be published, reproduced, copied or stored in a data processing system or circulated in any form by print, photo print, microfilm or any other means without written permission by EXIN.