

Exam requirements

Information Security Management Advanced based on ISO/IEC 27002 (ISMAS.EN)

Publication date	01-1-2010	
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.</p> <p>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>The module Information Security Management Advanced based on ISO/IEC 27002 (ISMAS.EN) tests organizational and managerial aspects of information security.</p> <p>The international standard, the Code of Practice for Information Security ISO/IEC 27002:2005 structures the organization of information security. For that reason, it is an important point of departure for this module.</p>	
Target group	<p>Starting professionals. This module is intended for everyone who through their position is involved in, for example, the implementation, evaluation and reporting of information security, such as the Information Security Manager (ISM) and the Information Security Officer (ISO) or the Line Manager and the Project Manager.</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	<p>Information Security Foundation based on ISO/IEC 27002 (ISFS.EN) or equivalent knowledge obtained in another way.</p>	
Practical assignment	Not applicable	
Examination details	Examination type:	Computer-based or paper-based multiple-choice
	Time allotted for examination:	90 minutes

Number of multiple-choice questions:	30
Pass mark:	65 % (20 out of 30)
Open book:	no
Electronic equipment permitted:	no

Sample questions A sample exam is available through your Accredited Training Provider.

Exam requirements	1. Information security policy and information security plan	(20%)
	2. Organization of information security	(30%)
	3. Risk analysis	(15%)
	4. Standards	(10%)
	5. Compliance	(15%)
	6. Evaluation	(10%)

Specification of the exam requirements

1. Information security policy and information security plan	1.1	Information security policy (15%)
	1.2	Information security plan (5%)
2. Organization of information security	2.1	Design of information security (22%)
	2.2	Functions in information security (8%)
3. Risk analysis	3.1	Classification of information and management of capital assets (7.5%)
	3.2	Risk analysis methods (7.5%)
4. Standards	2.1	Standards (2.5%)
	2.2	ISO/IEC 27001 and 27002 (7.5%)
5. Compliance	5.1	Legislation and regulations (5%)
	5.2	Protection of personal data (5%)
	5.3	Agreements and contracts (5%)
6. Evaluation	6.1	Quick scan (2.5%)
	6.2	Audit (7.5%)

Basic concepts

In Literature A, Peltier, Peltier and Blackley, an extended list of concepts can be found. The concepts used in Chapters 6 and 7 are not relevant.

Additional concepts in Literature B, ISO/IEC 27002:2005 (EN), the candidate should be familiar with:

- International Electrotechnical Commission (IEC)
- International Organization for Standardization (ISO)

Literature

- A. Peltier, Thomas R., Justin Peltier and John Blackley
Information Security Fundamentals
CRC Press LLC, 2005
ISBN 0-8493-1957-9
- B. **ISO/IEC 27002:2005 (EN)**
Information technology – Security techniques – Code of practice for information security management
Switzerland, ISO/IEC, 2005
www.iso.org
- C. Office of the Data Protection Commissioner, Ireland
Data Protection Checklist
<http://www.dataprotection.ie/ViewDoc.asp?fn=/documents/responsibilities/3k.htm&CatID=55&m=y>
- D. Federal Financial Institutions Examination Council (FFIEC)
Audit (Online IT Booklet)
http://www.ffiec.gov/ffiecinfobase/booklets/audit/audit_toc.htm

Additional Literature

Clinch, J.
ITIL V3 and Information Security
OGC White Paper May 2009
http://www.best-management-practice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf

Cazemier, Jacques A., Paul Overbeek and Louk Peters
Security Management Best Practice
Van Haren, January 2010
ISBN 978-90-8753-548 3

ISO/IEC 27000:2009 (EN)
Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
Switzerland, ISO/IEC, 2009
www.iso.org

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.