ISO 27000 Information Security Management Systems Foundation

Syllabus

November 2012

Version 01.3

www.peoplecert.org

PEOPLECERT

The Experts in certifying Professionals e-mail: info@peoplecert.org, www.peoplecert.org

1. Introduction

The **ISO/IEC 27000 series** of standards has been specifically reserved by ISO for information security matters and is a globally-recognized set of standards that outlines best practices in information security for an organization. The 27000 series is populated with a range of individual standards and documents. The emergence of **the ISO/IEC 27000 series of standards** is an extremely important development and is re-shaping approaches to information security on a global basis. For the purpose of this certification, two standards of the ISO/IEC 27000 series of standards will be used, and namely **ISO/IEC 27001: Information Security Techniques – Information Security Management Systems – Requirements (ISMS)** which is the recognized International standard, that provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) and **ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management.**

Information Security (IS) is becoming increasingly and rapidly more important to organizations. In addition, globalization of the economy leads to a growing exchange of information between organizations – from all perspectives including employees, customers, suppliers etc. – with a growing use of networks (internally and externally). This means that a lot of organization activities rely heavily on ICT, while information has become one of the most valuable assets of any organization, the security and the protection of this information being crucial for the continuity and effectiveness of the organization. The ISO/IEC 27001 and 27002 standards for Information Security Management allow an organization to demonstrate achievement of excellence and compliance with global best practices for quality in Information Security Management.

PEOPLECERT's ISO 27000 Foundation level qualification covers the **knowledge** required for a candidate to prove a solid understanding of the content and requirements of the international standard, specifically for **ISO/IEC 27001 and ISO/IEC 27002.** In short, the Foundation certification covers the knowledge required to gain an **understanding** of the **content** and **requirements** of the ISO/IEC 27000 international series of standards for the two specified standards in relation to Information Security Management. Other available levels of certification cover more advanced knowledge and application of the standard.

2. Target Group/Audience

This qualification is the **first level** of the ISO/IEC 27000 certification scheme provided by PEOPLECERT, and is aimed at anyone working within an organization (internally or externally) who may require to have and demonstrate a solid **knowledge** and **understanding** of the **ISO/IEC 27001** and **ISO/IEC 27002 standards** and their **content**. The certification can also cater for candidates seeking personal certification, also in regards to their knowledge and understanding of the requirements and the content of the standard.

This qualification will provide the **Foundation** level of knowledge to its holders and will certify that they have a solid understanding of the standard and its content.

Note that this qualification **does not** provide the **advanced** level of knowledge for:

(a) staff responsible for managing implementation of the standard in an organization
(b) external auditors
(c) external consultants or managers

This advanced level of knowledge is covered in the next levels of the ISO/IEC 27000 certification scheme provided by PEOPLECERT.

3. Learning Objectives

As this is the **Foundation** level course, candidates will be introduced to the principles and core elements of the ISO/IEC 27001 and ISO/IEC 27002 standards for Information Security Management, and more specifically:

- **ISO/IEC 27000:** which provides an overview of information security management systems, which form the subject of the ISMS family of standards, and defines related terms.
- **ISO/IEC 27001**: the formal specification which defines the requirements that must be achieved for an information security management system (ISMS).
- **ISO/IEC 27002:** which describes a code of practice for information security management and details hundreds of specific controls which may be applied to secure information and related assets.

Holders of **PEOPLECERT's ISO 27000**: Information Security Management **Foundation** Certification will be able to demonstrate their knowledge, ability, competence and understanding in:

- Definitions and principles of quality management services in accordance with ISO/IEC 27001.
- Positioning of ISO/IEC 20000 in the Information security management including its relationship with other standards and best practices.
- Objectives and requirements in each section of the specification.
- Scope, aims and use of the ISO/IEC 27001 and ISO/IEC 27002 Specification and Code of Practice.
- Processes and objectives of ISO/IEC 27001 and ISO/IEC 27002 and Information security management (ISMS).
- Fundamental requirements for an Information Security Management System (ISMS).
- Requirements of the Information Security Management System and the Plan, Do, Check, Act cycle.
- How assessments, reviews and internal audits of Information Security Management systems against the requirements of the standard are used.

4. Examination

The ISO/IEC 27000 Foundation Certification Exam is designed to validate a candidate's knowledge of the contents and requirements of the standard and will allow for further development along the ISO/IEC 27000 – Information Security Management certification path. The exam focuses on the following two categories in the cognitive domain of **Bloom's taxonomy**[1]:

- **Knowledge**
- **Comprehension**

4.1 Entry Criteria/Training Requirements

No specific entry criteria exist for candidates of the ISO/IEC 27000 Foundation level examination. However, it is strongly recommended that candidates have at least a basic knowledge of Information security management concepts and terminology and have undergone some formal training on the subject with a proposed duration of **24 hours**. ITIL® Foundation training is also recommended. A detailed breakdown of these training hours, per topic area is provided in the syllabus section.

[1] *The Bloom's taxonomy defines **six** (6) levels of learning in the **cognitive** domain (know, comprehend, apply, analyze, evaluate, create), which are both sequential and cumulative and move from the simple to the complex. In order to achieve the 6th level of learning, it must be ensured that the previous five levels have been mastered.*

4.2 Assessment Approach

The assessment approach used focuses on the basic categories of Knowledge and Comprehension.

Knowledge is defined as recalling previously learned material, from facts to theories and represents the lowest level of learning outcomes in the cognitive domain. Such learning outcomes are turned in assessment objectives that include knowing and recalling such as:

- Common and/or basic terms, definitions, concepts and principles
- Specific compliance requirements and facts
- Processes, procedures and assessment methods.

Comprehension is the lowest level of understanding and entails the ability to grasp the meaning of the material taught, including some sort of interpretation, translation or estimation during the process. Such learning outcomes and in turn assessment objectives go beyond simply recalling information and may include:

- Understanding facts, concepts and principles
- Interpreting material (i.e. charts, graphs, text)
- Justifying a process, procedure and assessment method.

The assessment incorporates the above learning outcomes as it uses assessment objectives that cater for the above cognitive domain categories.

4.3 Examination Format

The following table details the examination format:

Delivery	**Computer (web) or Paper based**
Type	**40 Multiple choice questions** *Single answer, one of four possible answers* *Each question is awarded one (1) mark*
Duration	**1 hour (60 minutes)** *For non-native speakers or candidates with a disability, an additional 15 minutes of extra time is allowed.*
Pass Mark	**65% (26/40)**
Invigilator / Supervisor / Proctor	**Yes** *Physical or Web proctoring*
Open Book	**No** *No materials are allowed in the examination room*
Prerequisites	**None**
Distinction	**N/A**

The tests are derived from a regularly updated question test bank (QTB) based on the test specification detailed below. Questions are used interchangeably among test sets. The overall difficulty level of each test is the same with any other test. A candidate is never assigned the same test in the case of multiple examination attempts.

4.4 Detailed Syllabus

The syllabus contains references to the established ISO/IEC 27001 and is structured into sections relating to **major subject headings** and numbered with a single digit section number. The **recommended training hours, per Syllabus Category** are also provided in this table. Note that for the Foundation level of certification all questions pertaining to the Knowledge set are **knowledge** and **understanding** items (level 1 & 2 only).
At the end of the training session, allow **30 minutes** for the candidates to familiarize themselves with the exam process and the sample questions. An additional hour could be provided for the sample test and/or answering the sample test for better preparation of the exam.

Category	Ref	Knowledge Set
ISMS-7.1 Introduction	ISMS-7.1.1	Scope of ISO/IEC 27000 series of standards
	ISMS-7.1.2	Recognize industry standards/best practices in Service Management and Quality management systems, such as: ITIL®, SixSigma®, CobiT, ISO/IEC 9000, ISO/IEC 20000
	ISMS-7.1.3	Recognize the content and correlation between ISO/IEC 27001:2005 and ISO/IEC 27002:2005
	ISMS-7.1.4	Definition and need for Information Security and Information Security Management System (ISMS)
	ISMS-7.1.5	Importance of an Information Security Management System (ISMS)
	ISMS-7.1.6	Value and Reliability of Information
	ISMS-7.1.7	Benefits and Critical Success factors of an Information Security Management System (ISMS)
Proposed Training Time: 60 minutes		
ISMS-7.2 Organization of Information Security	ISMS-7.2.1	Management responsibility: • Management commitment • Resource management
	ISMS-7.2.2	Confidentiality agreements
	ISMS-7.2.3	Contact with authorities and with special interest parties
	ISMS-7.2.4	Independent review of information security
	ISMS-7.2.5	Addressing security when dealing with external parties
Proposed Training Time: 180 minutes		
ISMS-7.3 Information Security Management System	ISMS-7.3.1	Information Security Policy
	ISMS-7.3.2	General ISMS requirements
	ISMS-7.3.3	Structure of policies

Category	Ref	Knowledge Set
	ISMS-7.3.4	Establishing and managing the ISMS: • Establish the ISMS • Implement and operate the ISMS • Monitor and review the ISMS • Maintain and improve the ISMS
	ISMS-7.3.5	Documentation requirements • General • Control of documents • Control of records
	ISMS-7.3.6	Management review of the ISMS • General • Review input • Review output
	ISMS-7.3.7	ISMS improvement: • Continual improvement • Corrective action • Preventive action
Proposed Training Time: 300 minutes		
ISMS-7.4 ISMS Implementation	ISMS-7.4.1	Defining ISMS scope, boundaries and ISMS policy
	ISMS-7.4.2	Asset Management: • Responsibility for assets • Information classification
	ISMS-7.4.3	Risk Assessment and Treatment: • Assessing security risks • Treating security risks
	ISMS-7.4.4	Information security aspects of business continuity management
Proposed Training Time: 150 minutes		
ISMS-7.5 Human resources, physical and environmental security	ISMS-7.5.1	Human Resources Security: Prior to employment
	ISMS-7.5.2	Human Resources Security: During employment
	ISMS-7.5.3	Human Resources Security: Termination or change of employment
	ISMS-7.5.4	Physical and Environmental Security: Secure areas
	ISMS-7.5.5	Physical and Environmental Security: Equipment security
Proposed Training Time: 120 minutes		
ISMS-7.6 Communications and operations management	ISMS-7.6.1	Operational procedures and responsibilities
	ISMS-7.6.2	Third party service delivery management
	ISMS-7.6.3	System Planning and acceptance: • Capacity management • System acceptance
	ISMS-7.6.4	Protection against malicious and mobile code
	ISMS-7.6.5	Back-up
	ISMS-7.6.6	Network security management
	ISMS-7.6.7	Media handling

Category	Ref	Knowledge Set
	ISMS-7.6.8	Exchange of information
	ISMS-7.6.9	Electronic commerce services
	ISMS-7.6.10	Monitoring
Proposed Training Time: 120 minutes		
ISMS-7.7 Access Control	ISMS-7.7.1	Access control policy
	ISMS-7.7.2	User access management
	ISMS-7.7.3	User responsibilities
	ISMS-7.7.4	Network access control
	ISMS-7.7.5	Operating system access control
	ISMS-7.7.6	Application and information access control
	ISMS-7.7.7	Mobile computing and teleworking
Proposed Training Time: 120 minutes		
ISMS-7.8 Information systems acquisition, development and maintenance	ISMS-7.8.1	Security requirements of information systems
	ISMS-7.8.2	Correct processing in applications
	ISMS-7.8.3	Cryptographic controls
	ISMS-7.8.4	Security of system files
	ISMS-7.8.5	Security in development and support processes
	ISMS-7.8.6	Technical vulnerability management
Proposed Training Time: 120 minutes		
ISMS-7.9 Compliance	ISMS-7.9.1	Compliance with legal requirements
	ISMS-7.9.2	Compliance with security policies and standards, and technical compliance
	ISMS-7.9.3	Internal ISMS audits: • Define criteria, scope, frequency, method and audit procedures • Define roles and responsibilities of internal auditors • Ensure objective and impartial documentation • Plan audit activities • Follow up activities • Record keeping procedures
Proposed Training Time: 150 minutes		
ISMS 7.10 Information Security Incident Management	ISMS-7.10.1	Reporting information security events
	ISMS-7.10.2	Management of information security incidents and improvements
Proposed Training Time: 120 minutes		
Total Proposed Training Time: 24 hours		

4.5 Test Specification

The examination will consist of **ten** (**10**) sections with the following structure:

Category	Description	Exam (%)
1	ISMS-7.1 Introduction	10.0%
2	ISMS-7.2 Organization of Information Security	17.5%
3	ISMS-7.3 Information Security Management System	17.5%
4	ISMS-7.4 ISMS Implementation	12.5%
5	ISMS-7.5 Human resources, physical and environmental security	7.5%
6	ISMS-7.6 Communications and operations management	5.0%
7	ISMS-7.7 Access Control	7.5%
8	ISMS-7.8 Information systems acquisition, development and maintenance	5.0%
9	ISMS-7.9 Compliance	10.0%
10	ISMS 7.10 Information Security Incident Management	7.5%
	Total	100.0%

5. Recommended Reading

(i) ISO/IEC copy of series' standards for this certification/examination:

ISO/IEC 27000:2009 Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary. Switzerland, ISO, 2009.

ISO/IEC 27001:2005 Information Technology — Security Techniques — Information Security Management Systems — Requirements. Switzerland, ISO, 2005.

ISO/IEC 27002:2005 Information Technology — Security Techniques — Code of Practice for Information Security Management. Switzerland, ISO, 2005

ISO/IEC 27003:2005 Information Technology — Security techniques — Information Security Management System Implementation Guidance. Switzerland, ISO, 2010

ISO/IEC 27004:2009 Information Technology — Security Techniques — Information Security Management - Measurement. Switzerland, ISO, 2009

(ii) ISO/IEC 20000-1:2005 Information Technology – Service Management – Part 1: Specification. Switzerland, ISO, 2005.

(iii) Calder, Alan. The Case for ISO 27001. IT Governance Publishing, 2005.

(iv) Calder, Alan. ISO27001/ISO27002 A Pocket Guide. IT Governance Publishing, 2008.

(v) Calder, Alan. Nine Steps to Success: an ISO 27001 Implementation Overview. IT Governance Publishing, 2006.

(vi) Calder, Alan and Steve G. Watkins. International IT Governance: An Executive Guide to ISO 17799/ISO 27001. USA: Kogan Press, 2006.

(vii) Calder, Alan and Steve G. Watkins. Information Security Risk Management for ISO27001/ISO27002. IT Governance Publishing, 2010.

(viii) Hintzbergen, J., Hintzbergen, K., Smulders, A. and Baars, H. Foundations of Information Security – Based on ISO27001 and ISO27002. Netherlands: Van Haren Publishing, 2010.

(ix) Watkins, Steve G. An Introduction to Information Security and ISO27001. IT Governance Publishing, 2008.

6. Glossary

Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements.
Accountability	Responsibility of an entity for its actions and decisions.
Accreditation Body	Assessment organizations that provide certification, testing, and inspection and calibration services. Accreditation by an accreditation body demonstrated competence, impartiality and performance capability of an organization that does audits. Ensures a consistent approach.
Accredited Certification Body	Organization that performs certification audits, commonly referred to as 'professional audit companies' and which has been accredited by an accreditation body.
Analytical model	Algorithm or calculation combining one or more base and/or derived measures with associated decision criteria [ISO/IEC 15939:2007].
Attribute	Property or characteristic of an object that can be distinguished quantitatively or qualitatively by human or automated means [ISO/IEC 15939:2007].
Asset	Anything that has value to the organization [ISO/IEC 13335-1:2004].
Attack	Attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset.
Authentication	Provision of assurance that a claimed characteristic of an entity is correct.
Authenticity	Property that an entity is what it claims to be.
Availability	The property of being accessible and usable upon demand by an authorized entity.
Business continuity	Processes and/or procedures for ensuring continued business operations.
Code of Practice	A standard that recommends 'good, accepted practice as followed by competent practitioners'.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Control	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
Control objective	Statement describing what is to be achieved as a result of implementing controls.
Corrective action	Action to eliminate the cause of a detected nonconformity or other undesirable situation.
Effectiveness	Extent to which planned activities are realized and planned results achieved.
Efficiency	Relationship between the results achieved and how well the resources have been used.
Event	Occurrence of a particular set of circumstances.
Facilities	Any information processing system, service or infrastructure, or the physical locations housing them.
Guideline	A description that clarifies what should be done and how, to achieve the objectives set out in policies.
Impact	Adverse change to the level of business objectives achieved.
Incident	Any event which is not part of the standard operation of a service and which causes or may cause an interruption to, or a reduction in, the quality of that service.
Indicator	Measure that provides an estimate or evaluation of specified attributes derived from an analytical model with respect to defined information needs.
Information asset	Knowledge or data that has value to the organization
Information processing facilities	Any information processing system, service or infrastructure, or the physical locations housing them.
Information security	Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
Information security event	An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information security	A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business

incident	operations and threatening information security [ISO/IEC TR 18044:2004].
Information security incident management	Processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents.
Information security management system ISMS	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
Information security risk	Potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization.
Integrity	The property of safeguarding the accuracy and completeness of assets.
Management system	framework of policies, procedures, guidelines and associated resources to achieve the objectives of the organization
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.
Policy	Overall intention and direction as formally expressed by management.
Preventive action	Action to eliminate the cause of a potential nonconformity or other undesirable potential situation.
Problem	Unknown underlying cause of one or more incidents.
Procedure	Specified way to carry out an activity or a process [ISO 9000:2005].
Process	Set of interrelated or interacting activities which transform inputs into outputs.
Record	Document stating results achieved or providing evidence of activities performed.
Reliability	Property of consistent intended behavior and results.
Residual risk	The risk remaining after risk treatment.
Risk	Combination of the probability of an event and its consequence.
Risk acceptance	Decision to accept a risk.
Risk analysis	Systematic use of information to identify sources and to estimate the risk.
Risk assessment	Overall process of risk analysis and risk evaluation.
Risk communication	Exchange or sharing of information about risk between the decision-maker and other stakeholders.
Risk criteria	Terms of reference by which the significance of risk is assessed.
Risk estimation	Activity to assign values to the probability and consequences of a risk.
Risk evaluation	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Risk treatment	Process of selection and implementation of measures to modify risk.
Specification	A standard that sets out 'detailed requirements', using the prescriptive 'shall', to be satisfied by a product, material process or system.
Statement of applicability	Documented statement describing the control objectives and controls that are relevant and applicable to the organization's ISMS.
Third party	A person or body that is recognized as being independent of the parties involved, as concerns the issue in question.
Threat	A potential cause of an unwanted incident, which may result in harm to a system or organization.
Vulnerability	A weakness of an asset or group of assets that can be exploited by one or more threats.