Information Security Management Qualification using ISO/IEC 27001

Supplementary reference paper

for ISO/IEC 27001 Foundation and Practitioner qualifications
April 2014

Document History

Version	Date	Updates made	Issued by
1.0	28 Nov 2012	1st issue	Andrew Marlow
2.0	20 March 2014	1. Updated for the 2013 edition of ISO/IEC 27001, 27002 and the 2014 edition of ISO/IEC 27000 2. Updated to fit with the revised ISO/IEC 27001 Foundation syllabus V2.0 3. Updated to fit with the newly launched ISO/IEC 27001 Practitioner qualification	Andrew Marlow

1 Introduction

Note: in the following text, 'ISMS' refers to an information security management system for ISO/IEC 27001.

This supplementary reference paper includes information which is referenced in the syllabus document for the Foundation and Practitioner ISO/IEC 27001 qualifications. This information is supplementary to and needs to be read in conjunction with other reference material which is defined in the syllabus for the qualification.

The target audience for this document is:

- APMG exam panel
- APMG exam board
- APMG assessment team
- Accredited Training Organizations (ATOs)
- Delegates of the ISO/IEC 27001 Foundation and Practitioner qualifications

2 Overview - supplementary information

2.1 Compatibility of ISMS with other management system standards, specifically ISO 9001 for quality management (Foundation OV0102)

ISO/IEC 27013 provides information as follows:

- Many organizations achieve certification to both ISO 9001 and ISO/IEC 27001
- It is possible to develop an integrated management system for both standards

2.2 Compatibility of ISMS with other management system standards, specifically ISO/IEC 20000-1 for service management (Foundation OV0103)

ISO/IEC 27013 provides information as follows:

- Many organizations achieve certification to both ISO/IEC 27001 and ISO/IEC 20000-1
- It is possible to develop an integrated management system for both standards
- It is important to note that the information security management process in ISO/IEC 20000-1 is a subset of ISO/IEC 27001. It also contains some requirements that are not in ISO/IEC 27001
- There are some differences in terminology and the handling of information security incidents
- ISO/IEC 27013 provides guidance on the integration of ISO/IEC 27001 and ISO/IEC 20000-1

2.3 Definitions (Foundation OV0104 and general usage in the practitioner paper)

The following terms and definitions from ISO/IEC 27000:2012 are useful as they are not defined in ISO/IEC 27000:2014:

Asset - Anything that has value to the organization

NOTE: There are many types of assets, including:
a) Information;
b) Software, such as a computer program;
c) Physical, such as computer;
d) Services;
e) People, and their qualifications, skills, and experience; and
f) Intangibles, such as reputation and image.

Information security management system
ISMS - Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

2.4 The APMG qualification scheme and the principles of ISO/IEC 27001 certification schemes (Foundation OV0108)

Source of information: ITSMF pocket guide, Planning and achieving ISO/IEC 20000 certification. The same principles apply to ISO/IEC 27001.

- Qualification schemes are for individuals. A qualification scheme provides the syllabus and examinations for ATOs and delegates. This qualification will cover details of the APMG scheme. The APMG qualification scheme has examinations at Foundation and Practitioner level. There are also other schemes operated by other organizations.
- Certification schemes are for organizations. There are several ISO/IEC 27001 certification schemes around the world. The certification schemes allow organizations to be certified to ISO/IEC 27001 after being independently assessed by a CB (Certification Body) for meeting all of the requirements of ISO/IEC 27001.
- According to ISO/IEC 17021, external audits for certification have 2 stages:
    - Document review, on-site or remote
    - On-site audit

2.5 The roles and responsibilities of the organizations and entities involved in ISO/IEC 27001 Qualification and Certification Schemes (FoundationOV0202)

Source of information: ITSMF pocket guide, Planning and achieving ISO/IEC 20000 certification. The same principles apply to ISO/IEC 27001.

a) APMG International

- Owns, manages and operates the APMG International ISO/IEC 27001 qualification scheme worldwide
- Accredits ATOs for the qualification scheme

b) Certification Bodies (CBs)

- Employ auditors who carry out formal assessments against ISO/IEC 27001 for organizations wishing to achieve certification under a certification scheme
- The CB is registered under certification schemes to demonstrate auditor independence and competence in ISMS
- CBs check and approve applications for audit and scope definitions for organizations
- CBs issue certificates to organizations who have been assessed as meeting the requirements of ISO/IEC 27001
- CBs may not provide guidance and consultancy to organizations where they are also acting as auditors
- CBs can perform a readiness assessment to look at readiness for certification
- CBs can provide training. This is usually in topics such as internal auditing or lead auditor but can also cover an overview of ISO/IEC 27001

c) National Accreditation Bodies (NABs)

- NABs oversee the operation of Certification Bodies in their geography and ensure that they meet requirements of relevant national and international standards
- To be accredited, CBs must be accredited by their NAB to confirm their competence as a certification body. They will then be known as an Accredited Certification Body (ACB)

d) Accredited Training Organizations (ATOs)

- The ATO, its trainers and courses are accredited by APMG under the APMG qualification scheme to provide training based on ISO/IEC 27001
- ATOs are subject to regular audit under the qualification scheme by APMG

e) Practitioner

- Practitioner is a generic term for individuals involved in carrying out aspects of the many activities in information security management. They can be involved in the planning, design, transition and operation of an ISMS that satisfies the requirements of ISO/IEC 27001. Examples are manager for an ISO/IEC 27001 implementation project, process owner, asset manager

f) Consultant

- Consultants are external experts who assist organizations in their development and improvement of an ISMS and achievements of certification to ISO/IEC 27001

g) Internal Auditor

- Auditors within an organization are known as internal auditors
- Internal auditors conduct audits of the ISMS within their own organization
- Internal auditors must demonstrate objectivity and impartiality (usually done by not auditing their own work)
- Practitioners and consultants may act as an internal auditor on behalf of an organization
- Internal auditors speak to the organization's staff and may additionally speak to customers, suppliers and internal groups to gather evidence

h) External Auditor

- Conduct formal audits on behalf of a CB
- CB auditors will only speak to the organization's staff, or other parties within the ISMS scope acting on behalf of the organization, to gather evidence, not to suppliers or other staff external to the scope of the ISMS
- Practitioners and consultants may act as an external auditor on behalf of a CB but may not audit their own work

3 Information security controls – supplementary information

3.1 The structure and contents of the controls and control objectives listed in Annex A of ISO/IEC 27001 (Foundation CO0101)

ISO/IEC 27002, 4 states that 'ISO/IEC 27001 contains 14 security control clauses collectively containing a total of 35 main security categories and 144 controls'.

(Note that the introduction to Annex A in ISO/IEC 27001 refers to Clause 6.1.3. To be exact, 6.1.3 is a sub-sub-clause).

There are 14 security control clauses.

Each security control clause is split into one or more security categories, each with a control objective.

Each security category is split into one or more controls which have a name and a description.

As an example, A.5 from ISO/IEC 27001 is shown with the names of each item in **BOLD CAPITAL**.

A.5 Information security policies. **SECURITY CONTROL CLAUSE**		
A.5.1 Management direction for information security. **SECURITY CATEGORY** *Objective:* To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. **CONTROL OBJECTIVE**		
A.5.1.1	Policies for information security **CONTROL NAME**	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties. **CONTROL DESCRIPTION**
A.5.1.2	Review of the policies for information security **CONTROL NAME**	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy and effectiveness. **CONTROL DESCRIPTION**

4 Achieving ISO/IEC 27001 Certification – supplementary information

4.1 The types of audits (Foundation AC0101, AC0201, AC0202)

The sources of information are ISO 19011, ISO/IEC 17000 and ISO/IEC 17021.

Type of Audit	Description
Initial certification audit	Conducted by a CB to do the first assessment of conformity against ISO/IEC 27001. In typical certification schemes, the certificate issued following a successful outcome lasts for 3 years.
Re-certification audit	Conducted by a CB after 3 years to do a further full assessment of conformity against ISO/IEC 27001 in typical certification schemes, In typical certification schemes, the certificate issued following a successful outcome lasts for 3 years.

Type of Audit	Description
Surveillance audit	Conducted by a CB and carried out at least annually to assess and ensure continued conformity. It ensures that representative areas of the management system are monitored on a regular basis. This is a shorter audit than the initial and re-certification audits. It focuses on improvements, internal audits, management review, complaints, operational control, effectiveness of the ISMS against information security objectives, areas of major change and any weaknesses identified during the previous audit
Internal audit	See first party audit below. An internal audit will meet the requirements of Clause 9.2 for ISO/IEC 27001
First party audit	Audit using the organization's own resources, or external consultants acting on their behalf, usually referred to as an internal audit
Second party audit	Audit by a person or organization that has a user interest in the organization e.g. customer
Third party audit	Audit by a conformity assessment organization usually referred to as a certification body. They are independent of and have no user interest in the organization

4.2 The outcomes of an audit (Foundation AC0102)

The outcomes, from ISO/IEC 17021, are identified by external and internal auditors.

a) Conformity

- Defined term in ISO/IEC 27000 as 'fulfilment of a requirement'
- The requirements of ISO/IEC 27001 have been met

b) Nonconformity

- Defined term in ISO/IEC 27000 as 'non-fulfilment of a requirement'
- Nonconformities can be graded into minor and major
- A major nonconformity is a failure to fulfill one or more requirements of ISO/IEC 27001 or a situation that raises significant doubt about the ability of the organization's management system to achieve its intended outputs. For example, management reviews are not held
- All other nonconformities are minor. For example, two documents are found with the wrong version number but all other documents are correct
- Nonconformities are recorded against a specific requirement in ISO/IEC 27001 and must have supporting evidence

c) Observation

- A conformity to the standard where there is an opportunity for improvement
- An observation is a recommendation for improvement but does not have to be auctioned

d) Outside of the audit scope

- An area which is not in the scope of the standard and therefore does not need to be audited

4.3 The evidence used to demonstrate conformity to ISO/IEC 27001 (Foundation AC0203)

The main audit evidence is in the form of documented information which is required in ISO/IEC 27001, 7.5. Documented information is defined in ISO/IEC 27000, 2.23 as:

Documented information

Information required to be controlled and maintained by an *organization* (2.57) and the medium on which it is contained

Note 1 to entry: Documented information can be in any format and media and from any source.

Note 2 to entry: Documented information can refer to

— the *management system* (2.46), including related *processes* (2.61);

— information created in order for the organization to operate (documentation);

— evidence of results achieved (records).

Audit evidence may be qualitative or quantitative (see ISO 19011) and must be verifiable. Some audit evidence may be collected by sampling.

Conformity must be shown to the requirements in ISO/IEC 27001:2013. In addition, for ISMS, there are requirements for certification in ISO/IEC 27006 which is aimed at CBs.

4.4 The organization's preparation for and participation in a certification audit (Foundation AC0204)

Based on ISO/IEC 17021, the organization's preparation for a certification audit covers the following activities:

- Agree applicability and scope with the auditor
- Agree dates with auditor
- Ensure locations and relevant staff are available
- Prepare logistics – rooms, security access for the auditor, who will accompany the auditor at all stages etc.
- Prepare all documentation (documents and any requested records) for the stage 1 audit (unlikely to be needed for a surveillance audit)
- Ensure all records are readily available for the stage 2 audit
- Prepare staff for the audit
- Participate in the audit
- Undertake follow-up activities
- Maintain conformity including ensuring that internal audits, management reviews and improvements take place
- Consider extending scope which can be done at a surveillance or re-certification audit

4.5 The process used by an accredited certification body to conduct certification audits for ISMS (Foundation AC0205)

Based on ISO/IEC 17021, the auditor will:

- Initiate the audit by validating the applicability and scope, planning the locations to be visited, roles to be interviewed and number of days
- Agree dates in advance with organization

- Undertake stage 1 audit - document review
- Prepare on-site audit, taking into account findings of document review as well as scope
- Undertake stage 2 audit on-site. Methods of collecting evidence are interview, observation of activities and review of records.
- CB auditors will only speak to the organization's staff or other parties in the scope of the ISMS and acting on behalf of the organization. (Note that internal auditors may additionally want to speak to customers, suppliers and internal groups to gather evidence)
- Present audit findings along with dates for follow up on any nonconformities
    - Major nonconformities means the audit is failed and will need to be rescheduled
    - Minor nonconformities need an agreed action plan
- Prepare, approve and distribute the audit report
- Complete the audit and issuing of certificate if successful
- Conduct audit follow-up to review nonconformity actions

5 List of exemplified Roles and Responsibilities for Information Security (PractitionerLE0205, LE0302, LE0402)

This table is used for the practitioner paper in the LE syllabus area. This information is taken directly from ISO/IEC 27003:2010, Table B.1

Table B.1 — List of exemplified Roles and Responsibilities for Information Security

Role	Brief Description of Responsibility
Senior Management (e.g. COO, CEO,CSO and CFO)	For vision, strategic decisions and coordinates activities to direct and control the organization.
Line Managers	Has the top responsibility for organizational functions.
Chief Information Security Officer	Has the overall responsibility and governance for information security ensuring the correct handling of information assets.
Information Security Committee (member of)	Handling the information assets and has a leading role for the ISMS in the organization.
Information Security Planning Team (member of)	During operations while the ISMS is being established. The planning team works across departments and resolves conflicts until the ISMS is established.
Stakeholder	In the context of the other roles' descriptions concerning information security, the stakeholder is primarily here defined as persons/bodies outside the normal operations – such as the board, owners (both in terms of organizational owners if the organization is part of a group or a government organization, and/or direct owners such as shareholders in a private organization). Other examples of stakeholders could be affiliated companies, clients, suppliers or more public organizations such as governmental financial control agencies or relevant stock exchange, if the organization is listed.
System administrator	The system administrator is responsible for an IT system.
IT Manager	The manager of all IT resources (e.g. IT department Manager).

Role	Brief Description of Responsibility
Physical Security	The person responsible for the physical security, e.g. buildings etc., often referred to as a Facility Manager.
Risk Management	The person/persons responsible for the organization's risk management framework including risk evaluation, risk treatment and risk monitoring.
Legal Advisor	Many information security risks have legal aspects and the legal advisor is responsible for taking these into consideration.
Human Resources	The person/persons with overall responsibility for the staff.
Archive	All organizations have archives containing vital information that needs to be stored for the long term. The information may be located on multiple types of media and a specific person should be responsible for the security of this storage.
Personal Data	If required by national law, there may be a person responsible for being the contact for data inspection board or similar official organization that oversees personal integrity and privacy issues.
System developer	If an organization develops their own information systems, someone has the responsibility for this development.
Specialist / Expert	The specialists and experts responsible for some operations in an organization should be referred to in terms of their intention about ISMS matters as it relates to use in their specific fields.
External Consultant	External consultants can give advice based on their macroscopic points of view of an organization and industry experience. However, consultants may not have the depth knowledge of the organization and operations of the organization.
Employee / Staff / User	Each employee is equally responsible for maintaining information security in the workplace and in his/her environment.
Auditor	The auditor is responsible for assessing and evaluating the ISMS.
Trainer	The trainer implements training and awareness programs.
Local IT or IS responsible	In a larger organization there is often somebody in the local organization that has local responsibility for IT matters, and possibly for information security as well.
Champion (Influential Person)	This is not a responsible role as such, but in a larger organization it may be of great help in the implementing stage to have people who have a deep knowledge about the implementation of an ISMS and can support the understanding and reasons behind the implementation. They may influence the opinion in a positive way and may also be called "Ambassadors".

6 Define roles & responsibilities for the preliminary ISMS scope (PractitionerLE0204, LE0301, LE0401)

This section is used for the Practitioner paper in the LE syllabus area. This information is taken directly from ISO/IEC 27003, 5.3.2.

Activity

The overall roles and responsibilities for the preliminary ISMS scope should be defined.

Input

a) Output from Activity 5.3.1 Develop the preliminary ISMS scope
b) List of stakeholders who will benefit from results of the ISMS project.

Guidance

In order to execute the ISMS project, the role of an organization for the project should be determined. The role generally is different at each organization, because of the number of people dealing with information security. The organizational structure and resources for information security vary with the size, type and structure of the organization. For example, in a smaller organization, several roles may be carried out by the same person. However, management should explicitly identify the role (typically Chief Information Security Officer, Information Security Manager or similar) with overall responsibility for managing information security, and the staff should be assigned roles and responsibilities based on the skill required to perform the job. This is critical to ensure that the tasks are carried out efficiently and effectively.

The most important considerations in the definition of roles in information security management are:

a) Overall responsibility for the tasks remains at the management level,
b) One person (usually the Chief Information Security Officer) is appointed to promote and co-ordinate the information security process,
c) Each employee is equally responsible for his or her original task and for maintaining information security in the workplace and in the organization.

The roles for managing information security should work together; this may be facilitated by an Information Security Forum, or similar body.

Collaboration with appropriate business specialists should be undertaken (and documented) at all stages of the development, implementation, operation and maintenance of the ISMS.

Representatives from departments within the identified scope (such as risk management) are potential ISMS implementation team members. This team should be maintained at the smallest practical size for speed and effective use of resources. Such areas are not only those directly included in the ISMS scope, but also the indirect divisions, such as legal, risk management and administrative departments.

Output

The deliverable is a document or table describing the roles and responsibilities with the names and organization needed to successfully implement an ISMS.