Information Security Management Qualification using ISO/IEC 27001

Supplementary reference paper

for ISO/IEC 27001
Foundation
Practitioner - Information Security Officer and Auditor

March 2020

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
3.0	31 May 2018	1. Updated for the renaming of Practitioner to Practitioner - Information Security Officer 2. Updated due to the revision of ISO/IEC 27003	Andrew Marlow
3.1	12 March 2020	1. Updated for the launch of the Auditor 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, Practitioner - Information Security Officer and Auditor 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, Practitioner – Information Security Officer and Auditor 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 - Information Security Officer paper)

The following terms and definitions from ISO/IEC 27000:2012 are useful as they are not defined in ISO/IEC 27000:2018:

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 - Information Security Officer 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 – Information Security Officer

- 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.
- The Information Security Officer is defined by organisations in various countries as a practical implementation of a role that is actually not required in ISO/IEC 27001. Typically, an Information Security Officer is taking care of compliance, documentation, risk management, business continuity and related topics, including the relationship with the top management.

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)
- Information Security Officers 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
- Information Security Officers 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 27002:2013, 4 states that 'ISO/IEC 27001 contains 14 security control clauses collectively containing a total of 35 main security categories and 114 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 and Auditor AC0101, AC0201, AC0202, AC0203, AC0204 and AC0205)

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 and Auditor AC0102)

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

a) Conformity

- Defined term in ISO/IEC 27000:2018, 3.11 as 'fulfilment of a requirement'
- The requirements of ISO/IEC 27001 have been met

b) Nonconformity

- Defined term in ISO/IEC 27000:2018, 3.47 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 actioned

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 and Auditor 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 27000:2018, 3.19 as:

Documented information

Information required to be controlled and maintained by an *organization* (3.50) 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* (3.41), including related *processes* (3.54);

— information created in order for the organization (3.50) 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 and Auditor 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 and Auditor 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 Appropriate boundaries and scope of the interaction of Interested Parties (Practitioner - Information Security Officer LE0211)

This information is used for the Practitioner - Information Security Officer paper in the LE syllabus area. This information is taken directly from ISO/IEC 27003:2017, 4.2

4.2 Understanding the needs and expectations of interested parties
Required activity
The organization determines interested parties relevant to the ISMS and their requirements relevant to information security.

Explanation
Interested party is a defined term (see ISO/IEC 27000:2018, 3.37) that refers to persons or organizations that can affect, be affected by, or perceive themselves to be affected by a decision or activity of the organization. Interested parties can be found both outside and inside the organization and can have specific needs, expectations and requirements for the organization's information security.

External interested parties can include:

a) regulators and legislators;
b) shareholders including owners and investors;
c) suppliers including subcontractors, consultants, and outsourcing partners;
d) industry associations;
e) competitors;
f) customers and consumers; and
g) activist groups.

Internal interested parties can include:

h) decision makers including top management;
i) process owners, system owners, and information owners;
j) support functions such as IT or Human Resources;
k) employees and users; and
l) information security professionals.

The results of this activity are used in ISO/IEC 27001:2013, 4.3 and 6.1.

Guidance
The following steps should be taken:

— identify external interested parties;
— identify internal interested parties; and
— identify requirements of interested parties.

As the needs, expectations and requirement of interested parties change over time, these changes and their influence on the scope, constraints and requirements of the ISMS should be reviewed regularly.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information
No other information.

6 Define roles & responsibilities for the preliminary ISMS scope (Practitioner: LE0204, LE0205, LE0301, LE0302, LE0401 & LE0402)

This section is used for the Practitioner - Information Security Officer paper in the LE syllabus area. This information is taken directly from ISO/IEC 27003:2017, 5.1 and 5.3

5.1 Leadership and commitment

Required activity
Top management demonstrates leadership and commitment with respect to the ISMS.

Explanation
Leadership and commitment are essential for an effective ISMS.

Top management is defined (see ISO/IEC 27000:2018, 3.75) as a person or group of people who directs and controls the organization of the ISMS at the highest level, i.e. top management has the overall responsibility for the ISMS. This means that top management directs the ISMS in a similar way to other areas in the organization, for example the way budgets are allocated and monitored. Top management can delegate authority in the organization and provide resources for actually performing activities related to information security and the ISMS, but it still retains overall responsibility.

As an example, the organization implementing and operating the ISMS can be a business unit within a larger organization. In this case, top management is the person or group of people that directs and controls that business unit.

Top management also participates in management review (see 9.3) and promotes continual improvement (see 10.2).

Guidance
Top management should provide leadership and show commitment through the following:

a) top management should ensure that the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization;

b) top management should ensure that ISMS requirements and controls are integrated into the organization’s processes. How this is achieved should be tailored to the specific context of the organization. For example, an organization that has designated process owners can delegate the responsibility to implement applicable requirements to these persons or group of people. Top management support can also be needed to overcome organizational resistance to changes in processes and controls;

c) top management should ensure the availability of resources for an effective ISMS. The resources are needed for the establishment of the ISMS, its implementation, maintenance and improvement, as well as for implementing information security controls.

Resources needed for the ISMS include:

1) financial resources;
2) personnel;
3) facilities; and
4) technical infrastructure.

The needed resources depend on the organization’s context, such as the size, the complexity, and internal and external requirements. The management review should provide information that indicates whether the resources are adequate for the organization;

d) top management should communicate the need for information security management in the organization and the need to conform to ISMS requirements. This can be done by giving practical examples that illustrate what the actual need is in the context of the organization and by communicating information security requirements;

e) top management should ensure that the ISMS achieves its intended outcome(s) by supporting the implementation of all information security management processes, and in particular through requesting and reviewing reports on the status and effectiveness of the ISMS (see 5.3 b)). Such reports can be derived from measurements (see 6.2 b) and 9.1 a)), management reviews and audit reports. Top management can also set performance objectives for key personnel involved with the ISMS;

f) top management should direct and support persons in the organization directly involved with information security and the ISMS. Failing to do this can have a negative impact on the effectiveness of the ISMS. Feedback from top management can include how planned activities are aligned to the strategic needs for the organization and also for prioritizing different activities in the ISMS;

g) top management should assess resource needs during management reviews and set objectives for continual improvement and for monitoring effectiveness of planned activities; and

h) top management should support persons to whom roles and responsibilities relating to information security management have been assigned, so that they are motivated and able to direct and support information security activities within their area.

In cases where the organization implementing and operating an ISMS is part of a larger organization, leadership and commitment can be improved by engagement with the person or group of people that controls and directs the larger organization. If they understand what is involved in implementing an ISMS, they can provide support for top management within the ISMS scope and help them provide leadership and demonstrate commitment to the ISMS. For example, if interested parties outside the scope of the ISMS are engaged in decision making concerning information security objectives and risk criteria and are kept aware of information security outcomes produced by the ISMS, their decisions regarding resource allocations can be aligned to the requirements of the ISMS.

Other information
No other information.

5.3 Organizational roles, responsibilities and authorities

Required activity

Top management ensures that responsibilities and authorities for roles relevant to information security are assigned and communicated throughout the organization.

Explanation

Top management ensures that roles and responsibilities as well as the necessary authorities relevant to information security are assigned and communicated.

The purpose of this requirement is to assign responsibilities and authorities to ensure conformance of the ISMS with the requirements of ISO/IEC 27001, and to ensure reporting on the performance of the ISMS to the top management.

Guidance

Top management should regularly ensure that the responsibilities and authorities for the ISMS are assigned so that the management system fulfils the requirements stated in ISO/IEC 27001.

Top management does not need to assign all roles, responsibilities and authorities, but it should adequately delegate authority to do this. Top management should approve major roles, responsibilities and authorities of the ISMS.

Responsibilities and authorities related to information security activities should be assigned. Activities include:

a) coordinating the establishment, implementation, maintenance, performance reporting, and improvement of the ISMS;
b) advising on information security risk assessment and treatment;
c) designing information security processes and systems;
d) setting standards concerning determination, configuration and operation of information security controls;
e) managing information security incidents; and
f) reviewing and auditing the ISMS.

Beyond the roles specifically related to information security, relevant information security responsibilities and authorities should be included within other roles.
For example, information security responsibilities can be incorporated in the roles of:

g) information owners;
h) process owners;
i) asset owners (e.g. application or infrastructure owners);
j) risk owners;
k) information security coordinating functions or persons (this particular role is normally a supporting role in the ISMS);
l) project managers;
m) line managers; and
n) information users.

Documented information on this activity and its outcome is mandatory only in the form and to the extent the organization determines as necessary for the effectiveness of its management system (see ISO/IEC 27001:2013, 7.5.1 b)).

Other information

No other information.