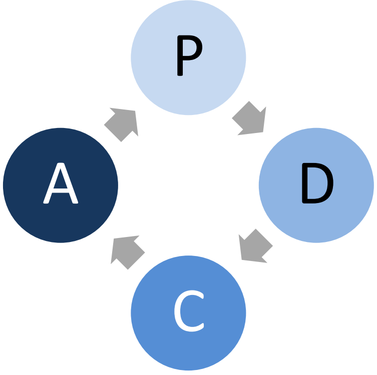
Qudos certification Limited
Level 30 The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AB, UK
w: qudoscert.com
e: info@qudoscert.com
t: +44 (0) 203 753 5558

October 2019

ISO 27001 Information Security & the PDCA cycle



It seems that every day another information security incident makes the news. Now, more and more organisations are implementing an ISMS (information security management system) to preserve the confidentiality, integrity and availability of their information.

Whilst there are several models that may be used as a basis for an ISMS, the ISO 27001 standard is fast becoming the industry-standard model in use. It is an international standard that specifies requirements for an ISMS and enables organisations to seek formal certification as an assurance to their clients and other interested parties.

The origins of ISO 27001 include the British standard BS 7799. The original ISO 27001 took an asset management approach, which has now evolved into a more risk-based approach in the current version.

The 2013 update of ISO 27001 was also one of the first ISO (International Standards Organisation) management system standards to be based on the new common high-level clause structure, and common terminology. The risk-based approach and new structure has also subsequently been applied to various other ‘new generation’ standards such as ISO 9001 (Quality management), ISO 14001 (environmental management), and ISO 45001 (OH&S management). Whilst individual standards may add additional “discipline-specific” requirements as required, ISO believes that this common approach will increase the value of such standards to users. It is particularly useful for those organisations that wish to implement an IMS (integrated management system) to address the requirements of two or more standards.

The following table illustrates the clause structure of ISO 27001:2013 in the context of the PDCA cycle – starting at clause 4 (the first clause specifying a requirement).

PLAN				DO	CHECK	ACT
4. Context of the organisation	**5. Leadership**	**6. Planning for the ISMS**	**7. Support**	**8. Operation**	**9. Performance evaluation**	**10. Improvement**
4.1 Understanding the organisation and its context	5.1 Leadership and commitment	6.1 Actions to address risks and opportunities	7.1 Resources	8.1 Operational planning and control	9.1 Monitoring, measurement, analysis and evaluation	10.1 Nonconformity and corrective action
4.2 Understanding the needs and expectations of interested parties	5.2 Policy	6.2 Information security objectives and planning to achieve them	7.2 Competence	8.2 Information security risk assessment	9.2 Internal audit	10.2 Continual improvement
4.3 Determining the scope of the ISMS	5.3 Organisational roles, responsibilities and authorities		7.3 Awareness	8.3 Information security risk treatment *Also, see Annex A	9.3 Management review	
4.4 Information security management system			7.4 Communication			
			7.5 Documented information			

Why do the listed clauses start at 4?

Well, naturally, ISO 27001's clauses do start at 1. However, clauses 1 to 3 refer to the scope of the standard, normative references, terms and definitions. As they don't specify any requirements, we haven't listed them here.

Annex A

In addition to the regular clauses, ISO 27001 includes **Annex A** which lists control objectives and controls to be considered and addressed as applicable. These objectives and controls form a major part of any ISMS based on that standard. By the way, the Annex A numbering system starts at 5 because of a relationship back to the clause numbering of ISO 27002 – which is a code of practice for information security controls.

A5 Information security policies	A12 Operation security
A6 Organisation of information security	A13 Communications security
A7 Human Resource security	A14 System acquisition, development and maintenance
A8 Asset management	A15 Supplier relationships
A9 Access control	A16 Information security incident management
A10 Cryptography	A17 Information security aspects of business continuity management
A11 Physical and environmental security	A18 Compliance

The following pages offer a brief summary of the clauses / controls and their requirements.

4 Context of the organisation

4.1 Understanding the organisation and its context.
4.2 Understanding the needs and expectations of interested parties.
4.3 Determining the scope of the ISMS.
4.4 Information security management system.

For the purposes of an ISMS, the context of the organisation are the internal and external factors that can affect the ability to preserve the confidentiality, integrity and availability of information. Understanding the context of an organisation might involve some form of situational awareness or PEST/SWOT analysis.

The relevant needs and expectations of clients and other interested parties need to be understood. That would, of course, include the legal and regulatory environment, and any contractual obligations. At that point, the scope and boundaries of the ISMS may be determined more holistically, and the necessary operational and support processes can be established.

5 Leadership

5.1 Leadership and commitment.
5.2 Policy.
5.3 Organisational roles, responsibilities and authorities.

For an ISMS to be successful, it needs to be inspired and led from the top. Top management must take accountability for it, express their commitment, give direction, and – critically – ensure that sufficient resources are made available.

Everyone in the organisation should be aware of what its policies and objectives are, and their role and responsibilities for achieving them.

In larger organisations, top management may not be able to attend to the day-to-day administration of the system themselves. Other people may perform those roles, but they **must** be given leadership, support, and adequate resources.

6 Planning for the ISMS

6.1 Actions to address risks and opportunities.
6.2 Information security objectives and planning to achieve them.
6.3 Planning of changes.

This clause is closely linked to clause 4. Having identified factors that affect information security, the organisation needs to develop strategies and actions to:

- Maintain and build on its **Strengths**
- Correct **Weaknesses** that might be barriers to meeting requirements and achieving objectives
- Grasp or maximise **Opportunities**
- Mitigate or manage **Threats or Risks**

There should be a 'Statement of applicability' to support these requirements, a risk assessment process and some form of Action Plan to address the risks and opportunities identified. That would include the controls listed in Annex A of the standard.

The organisation should put a programme in place to set measurable information security objectives, assign them, and monitor progress on them.

7 Support

7.1 Resources.
7.2 Competence.
7.3 Awareness.
7.4 Communication.
7.5 Documented information.

Determine, plan, and provide the resources and support mechanisms needed for the organisation to achieve its information security objectives.

People with responsibilities in the ISMS must be competent to the required level. When the required level in place, action must be taken to acquire it e.g. by training, education, recruitment or outsourcing.

People that work for the organisation must be aware of its ISMS policy, how they should contribute to the system, and any consequences of them not conforming to requirements.

The organisation needs to determine how it will communicate – both internally and externally – about matters relating to the ISMS.

The ISMS should be documented to the extent required for conformance to the various clauses / controls in the standard. The organisation should keep the required records.

8 Operations

8.1 Operational planning and control.
8.2 Information security risk assessment.
8.3 Information security risk treatment.

By virtue of this section the organisation is required to plan, implement and maintain the necessary people, process and technology controls that are required to address the information security risks that have been identified. A risk assessment should be performed on a periodic basis and the risk treatment planning should be similarly checked from time to time, in order to ensure that it is still effective and adequately meets the needs of the organisation.

Plan, implement and control the processes needed to meet information security requirements. This includes any processes that are outsourced.

Change management processes should be implemented.

9 Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation.
9.2 Internal audit.
9.3 Management review.

All systems need to be checked to verify that they are on track. Information Security Management Systems are no exception. Having implemented a system of controls over information security processes, organisations need to measure, monitor, and evaluate performance in meeting requirements and achieving objectives. Performance evaluation requirements may broadly be divided into these areas:

- Evaluate the performance of the information security system.
- Audit its effective implementation and conformance to requirements.
- Top management to periodically review the system.

10 Improvement

10.1 Nonconformity and corrective action.
10.2 Continual improvement.

The organisation will need to ensure that they deal with any nonconformities, determining the cause(s) and taking action to eliminate them and or to prevent reoccurrence in order to strive towards a continuous improvement model for the ISMS.

Continually improve the system to achieve objectives or increase the likelihood of achieving them. Also, seek opportunities to improve confidentiality, integrity and availability.

Annex controls

One thing that sets ISO 27001 apart from other ISO management systems standards is its Annex A. This specifies 114 controls over 14 sets or domains. Each dealing with a different aspect of information security. These controls are to be used in the context of the organisation's 'Statement of applicability'. They should address the relevant risks and opportunities that have been identified. There may be some overlaps between controls listed in the annex and requirements specified in the main body of the standard.

A5 Information security policies

Provide management direction and support for the implementation of the ISMS and to underpin commitment to the stated objectives of the organisation. This may include the need to define high level strategic policies as well as more detailed technical standards as applicable to the environment.

A6 Organisation of information security

Establish a framework for implementing and operating information security within the organisation. This includes defining roles and responsibilities, and – where necessary – segregating duties to minimise risks.

Establish policies and controls that will ensure the security related to remote working and use of mobile devices. For many organisations, this would include consideration of remote working (or teleworking) and a BYOD policy.

A7 Human resource security

Ensure that workers are aware of their responsibilities with regards to information security and ensure that they are fulfilling them.

In addition, these provisions require that workers are suitably qualified and experienced for their roles with regards to Information Security.

The organisation's also needs to confirm how information/data will be protected when workers change roles or if a person's employment is terminated.

A8 Asset management

The organisation is required to identify and record the information and data assets that it holds. This should include some form of data asset inventory or other asset register for ease of reference and to ensure accountability and ownership where required.

There is a requirement for a policy on the acceptable use of information, data and related organisational assets. This is an important communication requirement of the ISMS as it sets out the relative boundaries of what is deemed acceptable or normal use within the organisation.

Establish a system of data classification and provide guidance on how the labelling of such assets should be handled.

The organisation will also be required to declare that unauthorised disclosure should be prevented and reported where it occurs, this will also include the loss of such information/data stored on portable or disposable media.

A9 Access control

In this control, the organisation is required to restrict access to information/data and associated processing facilities to only those with a business need to know.

Only authorised users should be able to gain an appropriate level of access to systems and services – and in addition, measures should be in place to actively prevent any unauthorised access.

Users are required to be accountable for safeguarding their own authentication information, usually in the basic form of credentials (e.g. passwords) and there is a requirement to define the specific technical provisions which support such safeguarding, for example password complexity/strength requirements.

As this is normally a fundamental control objective within any ISMS, a formal policy is required.

A10 Cryptography

In order to reduce the ability of non-authorised persons and users from gaining access to sensitive information/data processed stored or transmitted by the organisation, it is likely that technical solutions which use cryptography will be required. Such provisions will help to protect the confidentiality and/or integrity of the information/data in question and this controls makes particular reference to other operational controls such as the management of cryptographic keys.

Again, as a fundamental control within the ISMS, a formal policy is required to support this control.

A11 Physical and environmental security

To further prevent unauthorised physical access to information/data held by the organisation and to avoid damage, theft or compromise of the assets and processing facilities, specific requirements are outlined within this important area of control. Such provisions may include the need for a clear desk / clear screen policy or a process for handling visitors.

A12 Operations security

In this somewhat expansive area of the standard, the organisation is required to ensure that a number of controls are considered for continued secure operations to be sustained, which include:

- Protection against malware (including viruses. Ransomware etc.).

- Change Management
- Separation of the environment between production and non-productions systems/data
- Provisions for backup and recovery of the environment
- Generation and collection of log events to identify and respond to any anomalies
- Performance of proactive vulnerability management activities
- Control of software installation

There is also mention of the requirement to minimise the impact of any audit and checking activities upon business operations, which given the extent of the requirements being applied to an existing environment can always be difficult to achieve.

A13 Communications security

This control area focuses on ensuring the protection of information/data across the network and seeks to maintain the security of information/data when it is processed or transmitted within the organisation or shared with any external parties.

A14 System acquisition, development and maintenance

In order to ensure that information security is an integral part of the procurement, development and ongoing maintenance of information systems across the organisation, this control requirement looks at what provisions need to be in place throughout the delivery lifecycle.

This includes requirements for information systems which provide services over public networks and to ensure that any data that might be used during delivery (e.g. for testing) is appropriately protected.

A15 Supplier relationships

This control section is intended to ensure that the protection of information/data assets that may be accessible by any external suppliers. This includes a requirement to ensure that control provisions are included within supplier agreements, to continuously monitor and manage supplier performance with regards to information security and also, to make sure that changes to the risk profile of any appointed supplier(s) is controlled.

A16 Information security incident management

The organisation is required to ensure that formal procedures are in place for the management of Information Security incidents. This should include details as to the main roles and responsibilities of staff with regards to incident management, the reporting of security events and weaknesses, how security incidents are responded to, the collection of evidence in relation to such events and how lessons learned are handled following an incident.

A17 Information security aspects of business continuity management

The organisation is required to establish the requirements for business continuity management in the event of a crisis or a disaster, such that it can respond effectively and efficiently. This includes the need for documented procedures to be in place and the need for periodic checking/testing of the provisions to ensure that they are fit for purpose and adequately address the risks identified.

A18 Compliance

This final control section seeks to ensure that the organisation avoids breaches of legal or other compliance obligations related to information security. In a broad sense, it includes the requirement for reviews of the ISMS using both internally and independent bodies, to observe claims to intellectual property/software licensing and also to comply with relevant data privacy regulations.

Your next step?

The above is just a broad outline of the standard and its requirements. The full standard includes much more detail and is available from your local standards association and other sources.

Further useful articles on ISO 27001 are included in the blog area of our web site.

Qudos and its partners can provide gap analysis and certification audit services for this and other standards in many countries throughout the world.

Contact us now to discuss your needs further.

Qudos certification Limited
Level 30 The Leadenhall Building, 122 Leadenhall Street, London EC3V 4AB, UK
w: qudoscert.com
e: info@qudoscert.com
t: +44 (0) 203 753 5558