Transition guide

Moving from ISO/IEC 27001:2005 to ISO/IEC 27001:2013

The new international standard for information security management systems

bsi.

...making excellence a habit.™

Successful businesses understand the value of timely, accurate information, good communications and secrecy. Information security is as much about exploiting the opportunities of our interconnected world as it is about risk management.

That's why organizations need robust information security management.

This guide has been designed to help you meet the requirements of the new international standard for information security management, ISO/IEC 27001:2013, which is the first revision of ISO/IEC 27001:2005.

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) for any organization, regardless of type or size. BSI recommends that every business has a system in place to maintain the confidentiality, integrity and availability of information. This will include its own information as well as customer information and other interested parties. In an ever increasing interconnected world the wisdom of doing this cannot be overestimated.

Meeting the requirements of the new international standard has never been easier. This guide is based on David Brewer's new books 'An introduction to ISO/IEC 27001:2013', which shares practical guidance on how to meet the requirements of ISO/IEC 27001:2013, and 'Understanding the new ISO management system requirements', which looks at management systems in general and how to transition them to the new standards. These books are available through the BSI shop.

This transition guide will help you understand the relationship between ISO/IEC 27001:2013 and its predecessor ISO/IEC 27001:2005 and the impact that the new standard is likely to have on your existing ISMS.

NB. *This transition guide is designed to be read in conjunction with BS ISO/IEC 27001:2013 — Information technology —Security techniques — Information security management systems — Requirements. It does not contain the complete content of the standard and should not be regarded as a primary source of reference in place of the standard itself.*

Why adopt an information security standard?

There are various reasons why organizations choose to have an information security management system (ISMS). These broadly fit broadly into two categories: market assurance and governance. Market assurance concerns the ability of an ISMS to provide confidence, within the marketplace, in an organization's ability to look after information securely. In particular, it inspires confidence that the organization will maintain the confidentiality, integrity and availability of customer information. Governance concerns how organizations are managed. In this case, an ISMS is recognized as being a proactive way to manage information security.

A typical scenario in the case of market assurance is when a company demands various assurances from its suppliers in order for them to continue as suppliers to that company. The norm used to be that such companies would require their suppliers to conform to ISO 9001, but now companies are also looking for assurances from their suppliers with regards to ISO/IEC 27001. In this case, the company will have a duty of due care to preserve the security of the information in its custody. If that information is shared with a supplier, then the company would be failing in its duty of care if the supplier's handling of that information was insecure. It doesn't matter whether the company chooses to do this for reasons of governance or market assurance, it only matters that it does

As the two categories are closely related, an organization may initially choose to have an ISMS in order to inspire confidence within the marketplace. Once it has its ISMS, as it matures, the people within the organization often experience the benefits of being able to better manage information security. Therefore the organization's reasons for having an ISMS may expand to cover both market assurance and governance. Likewise, another organization might start out by having an ISMS for better management. However, as its ISMS matures, it may communicate its experiences and news on successful certification audits to the marketplace and learn the power of market assurance to attract new customers.

Implementing ISO/IEC 27001

ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS. These requirements describe the intended behaviour of an ISMS once it is fully operational. The standard is not a step by step guide on how to build or create an ISMS.

However there are a number of books and other standards in the ISO/IEC 27000 series of standards which can assist. There are three core standards:

1. ISO/IEC 27003: Information technology —Security techniques — Information security management system implementation guidance;
2. ISO/IEC 27004, Information technology —Security techniques — Information security management — Measurement; and
3. ISO/IEC 27005, Information technology —Security techniques — Information security risk management.

All three guidance standards are currently being revised, and presently only address the requirements of ISO/IEC 27001:2005.

Comparing ISO/IEC 27001:2013 with ISO/IEC 27001:2005

ISO/IEC 27001:2013 is the first revision of ISO/IEC 27001. First and foremost, the revision has taken account of practical experience of using the standard: there are now over 17,000 registrations worldwide. However, there have been two other major influences on the revision. The first is an ISO requirement that all new and revised management system standards must conform to the high level structure and identical core text defined in Annex SL to Part 1 of the ISO/IEC Directives. Conformance to these requirements will have a tendency to make all management system standards look the same, with the intention that management system requirements that are not discipline-specific are identically worded in all management system standards. This is good news for organizations that operate integrated management systems, i.e. management systems that conform to several standards, such as ISO 9001 (quality), ISO 22301 (business continuity) as well as ISO/IEC 27001. The second influence was a decision to align ISO/IEC 27001 with the principles and guidance given in ISO 31000 (risk management). Again, this is good news for integrated management systems as now an organization may apply the same risk assessment methodology across several disciplines.

The result is that structurally ISO/IEC 27001:2013 looks very different to ISO/IEC 27001:2005.In addition, there are no duplicate requirements, and the requirements are phrased in a way, which allows greater freedom of choice on how to implement them. A good example of this is that the identification of assets, threats and vulnerabilities is no longer a prerequisite for the identification of information security risks. The standard now makes it clearer that controls are not to be selected from Annex A, but are determined through the process of risk treatment. Nevertheless, Annex A continues to serve as a cross-check to help ensure that no necessary controls have been overlooked.

New concepts have been introduced (or updated) as follows:

New/updated concept	Explanation
Context of the organization	The environment in which the organization operates
Issues, risks and opportunities	Replaces preventive action
Interested parities	Replaces stakeholders
Leadership	Requirements specific to top management
Communication	There are explicit requirements for both internal and external communications
Information security objectives	Information security objectives are now to be set at relevant functions and levels
Risk assessment	Identification of assets, threats and vulnerabilities is no longer a prerequisite for the identification of information security risks
Risk owner	Replaces asset owner
Risk treatment plan	The effectiveness of the risk treatment plan is now regarded as being more important than the effectiveness of controls
Controls	Controls are now determined during the process of risk treatment, rather than being selected from Annex A
Documented information	Replaces documents and records
Performance evaluation	Covers the measurement of ISMS and risk treatment plan effectiveness
Continual improvement	Methodologies other than Plan-Do-Check-Act (PDCA) may be used

Clause 0: Introduction

This is a much shorter clause than its predecessor. In particular the section on the PDCA model has been removed. The reason for this is that the requirement is for continual improvement (see Clause 10) and PDCA is just one approach to meeting that requirement. There are other approaches, and organizations are now free to use them if they wish.

The introduction also draws attention to the order in which requirements are presented, stating that the order does not reflect their importance or imply the order in which they are to be implemented.

Clause 1: Scope

This, too, is a much shorter clause. In particular there is no reference to the exclusion of controls in Annex A.

Clause 2: Normative references

The only normative reference is to ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary.

Clause 3: Terms and definitions

There are no longer any terms or definitions in ISO/IEC 27001:2013. Instead, readers are referred to ISO/IEC 27000. However, please ensure that you use a version of ISO/IEC 27000 that was published after ISO/IEC 27001:2013 otherwise it will not contain the correct terms or definitions. This is an important document to read. Many definitions, for example 'management system' and 'control' have been changed and now conform to the definitions given in the new ISO directives and ISO 31000. If a term is not defined in ISO/IEC 27000, please use the definition given in the Oxford English Dictionary. This is important, otherwise confusion and misunderstanding may be the result.

Clause 4: Context of the organization

This is a new clause that in part addresses the depreciated concept of preventive action and in part establishes the context for the ISMS. It meets these objectives by drawing together relevant external and internal issues (i.e. those that affect the organization's ability to achieve the intended outcome(s) of its ISMS) with the requirements of interested parties to determine the scope of the ISMS.

It should be noted that the term 'issue' covers not only problems, which would have been the subject of preventive action in the previous standard, but also important topics for the ISMS to address, such as any market assurance and governance goals that the organization might set for the ISMS. Further guidance is given in Clause 5.3 of ISO 31000:2009.

Note that the term 'requirement' is a 'need or expectation that is stated, generally implied or obligatory'. Combined with Clause 4.2, this in itself can be thought of as a governance requirement, as strictly speaking an ISMS that did not conform to generally-accepted public expectations could now be ruled nonconformant with the standard.

The final requirement (Clause 4.4) is to establish, implement, maintain and continually improve the ISMS in accordance with the requirements the standard.

Clause 5: Leadership

This clause places requirements on 'top management' which is the person or group of people who directs and controls the organization at the highest level. Note that if the organization that is the subject of the ISMS is part of a larger organization, then the term 'top management' refers to the smaller organization. The purpose of these requirements is to demonstrate leadership and commitment by leading from the top.

A particular responsibility of top management is to establish the information security policy, and the standard defines the characteristics and properties that the policy is to include.

Finally, the clause places requirements on top management to assign information security relevant responsibilities and authorities, highlighting two particular roles concerning ISMS conformance to ISO/IEC 27001 and reporting on ISMS performance.

Clause 6: Planning

Clause 6.1.1, General: This clause works with Clauses 4.1 and 4.2 to complete the new way of dealing with preventive actions. The first part of this clause (i.e. down to and including 6.1.1 c)) concerns risk assessment whilst Clause 6.1.1 d) concerns risk treatment. As the assessment and treatment of information security risk is dealt with in Clauses 6.1.2 and 6.1.3, then organizations could use this clause to consider ISMS risks and opportunities.

Clause 6.1.2, Information security risk assessment: This clause specifically concerns the assessment of information security risk. In aligning with the principles and guidance given in ISO 31000, this clause removes the identification of assets, threats and vulnerabilities as a prerequisite to risk identification. This widens the choice of risk assessment methods that an organization may use and still conforms to the standard. The clause also refers to 'risk assessment acceptance criteria', which allows criteria other than just a single level of risk. Risk acceptance criteria can now be expressed in terms other than levels, for example, the types of control used to treat risk.

The clause refers to 'risk owners' rather than 'asset owners' and later (in Clause 6.1.3 f)) requires their approval of the risk treatment plan and residual risks.

In other ways the clause closely resembles its counterpart in ISO/IEC 27001:2005 by requiring organizations to assess consequence, likelihood and levels of risk.

Clause 6.1.3, Information security risk treatment: This clause concerns the treatment of information security risk. It is similar to its counterpart in ISO/IEC 27001:2005, however, it refers to the 'determination' of necessary controls rather than selecting controls from Annex A. Nevertheless, the standard retains the use of Annex A as a cross-check to make sure that no necessary control has been overlooked, and organizations are still required to produce a Statement of Applicability (SOA). The formulation and approval of the risk treatment plan is now part of this clause.

Clause 6.2, Information security objectives and planning to achieve them: This clause concerns information security objectives. It uses the phrase "relevant functions and levels", where here, the term 'function' refers to the functions of the organization, and the term 'level', its levels of management, of which 'top management' is the highest. The clause defines the properties that an organization's information security objectives must possess.

Clause 7: Support

This clause begins with a requirement that organizations shall determine and provide the necessary resources to establish, implement, maintain and continually improve the ISMS. Simply expressed, this is a very powerful requirement covering all ISMS resource needs.

The clause continues with requirements for competence, awareness and communication, which are similar to their counterparts in ISO/IEC 27001:2005.

Finally, there are the requirements for 'documented information'. 'Documented information' is a new term that replaces the references in the 2005 standard to 'documents' and 'records'. These requirements relate to the creation and updating of documented information and to their control. The requirements are similar to their counterparts in ISO/IEC 27001:2005 for the control of documents and for the control of records.

Note that the requirements for documented information are presented in the clause to that they refer to. They are not summarized in a clause of their own, as they are in ISO/IEC 27001:2005.

Clause 8: Operation

This clause deals with the execution of the plans and processes that are the subject of previous clauses.

1. **Clause 8.1** deals with the execution of the actions determined in Clause 6.1, the achievement of the information security objectives and outsourced processes;
2. **Clause 8.2** deals with the performance of information security risk assessments at planned intervals, or when significant changes are proposed or occur; and
3. **Clause 8.3** deals with the implementation of the risk treatment plan.

Clause 9: Performance evaluation

Clause 9.1, Monitoring, measurement, analysis and evaluation: The first paragraph of Clause 9.1 states the overall goals of the clause. As a general recommendation, determine what information you need to evaluate the information security performance and the effectiveness of your ISMS. Work backwards from this 'information need' to determine what to measure and monitor, when, who and how. There is little point in monitoring and making measurements just because your organization has the capability of doing so. Only monitor and measure if it supports the requirement to evaluate information security performance and ISMS effectiveness.

Note that an organization may have several information needs, and these needs may change over time. For example, when an ISMS is relatively new, it may be important just to monitor the attendance at, say, information security awareness events. Once the intended rate has been achieved, the organization might look more towards the quality of the awareness event. It might do this by setting specific awareness objectives and determining the extent to which the attendees have understood what they have learnt. Later still, the information need may extend to determine what impact this level of awareness has on information security for the organization.

Clause 9.2, Internal audit: This clause is similar to its counterpart in ISO/IEC 27001:2005. However, the requirement holding management responsible for ensuring that audit actions are taken without undue delay has been removed, as it is effectively covered by the requirements in Clause 10.1 (in particular 10.1 a), c) and d)). The requirement that auditors shall not audit their own work has also been removed, as it is covered by the requirement to ensure objectivity and impartiality (Clause 9.2 e)).

Clause 9.3, Management review: Rather than specify precise inputs and outputs, this clause now places requirements on the topics for consideration during the review. The requirement for reviews to be held at planned intervals remains but the requirement to hold the reviews at least once per year has been dropped.

Clause 10: Improvement

Due to the new way of handling preventive actions, there are no preventive action requirements in this clause. However, there are some new corrective action requirements. The first is to react to nonconformities and take action, as applicable, to control and correct the nonconformity and deal with the consequences. The second is to determine whether similar nonconformities exist, or could potentially occur. Although the concept of preventive action has evolved there is still a need to consider potential nonconformities, albeit as a consequence of an actual nonconformity. There is also a new requirement to ensure that corrective actions are appropriate to the effects of the nonconformities encountered.

The requirement for continual improvement has been extended to cover the suitability and adequacy of the ISMS as well as its effectiveness, but it no longer specifies how an organization achieves this.

Annex A

The title of Annex A is now "reference control objectives and controls" and the introduction is simplified. It states that the control objectives and controls are directly derived from ISO/IEC 27002:2013 and that the Annex is to be used in the context of Clause 6.1.3.

During the revision of ISO/IEC 27002 the number of controls has been reduced from 133 controls to 114 controls, and the number of major clauses has been expanded from 11 to 14. Some controls are identical or otherwise very similar; some have been merged together; some have been deleted and some are new. For example:

1. A.5.1.1, Policies for information security is very similar to the original A.5.1.1, Information security policy document.
2. The old A.10.10.1, Audit logging, A.10.10.2, Monitoring of system use, and A.10.10.5, Fault logging, have been merged together to form the new A.12.4.1, Event logging.
3. The old A.11.6.2, Sensitive system isolation, has been removed on the grounds that in an interconnected world, such a control defeats the objective of being interconnected.
4. A.17.2.1, Availability of information processing facilities is a new control.

It is important to appreciate that the usefulness of a control to an organization should not change because it has been removed from Annex A. In accordance with Clause 6.1.3, controls are now determined on the basis of risk treatment. If an organization wishes to treat particular risks by deliberately not connecting a computer to the Internet or other networks, then it will need to use a control like the old A.11.6.2 regardless of whether it is in Annex A or not.

Annex A remains as a 'normative annex'. This is not because Annex A contains normative requirements but because, by ISO rules, it is referenced from a normative requirement, i.e. in this case, Clauses 6.1.3 c) and d).

Other annexes

The original Annex B, OECD principles and this international standard, has been dropped as it is now an old reference, which refers to PDCA.

The old Annex C, Correspondence between ISO 9001:2000, ISO 14001:2004 and this international standard, has also been dropped because both of these standards are being revised and will use the same high level structure and identical core text as ISO/IEC 27001:2013.

Annex B, Bibliography, of ISO/IEC 27001:2013 is an updated version of its counterpart, Annex D in ISO/IEC 27001:2005.

Documented information

The requirements for documented information are spread throughout the standard. However, in summary they are:

4.3	Scope of the ISMS
5.2	Information security policy
6.1.2	Information security risk assessment process
6.1.3	Information security risk treatment process
6.1.3 d)	Statement of Applicability
6.2	Information security objectives
7.2 d)	Evidence of competence
7.5.1 b)	Documented information determined by the organization as being necessary for the effectiveness of the ISMS
8.1	Operational planning and control
8.2	Results of the information security risk assessments
8.3	Results of the information security risk treatment
9.1	Evidence of the monitoring and measurement results
9.2 g)	Evidence of the audit programme(s) and the audit results
9.3	Evidence of the results of management reviews
10.1 f)	Evidence of the nature of the nonconformities and any subsequent actions taken
10.1 g)	Evidence of the results of any corrective action

Mapping tables

The following two tables illustrate the relationship between ISO/IEC 27001:2013 and ISO/IEC 27001:2005. Table A deals with the main body of the standard and Table B deals with Annex A. These are simplified tables for illustrative purpose only.

Table A lists the minor clause titles in ISO/IEC 27001:2013 in the left hand column. For each one, the entry in the right hand column shows the clause titles in ISO/IEC 27001:2005 that correspond in some way. In order to see exactly what is new and what has been removed, please consult the detailed mapping data.

Table A: Mapping of ISO/IEC 27001:2013 clauses to ISO/IEC 27001:2005

ISO/IEC 27001:2013		ISO/IEC 27001:2005	
0	Introduction	**0**	Introduction
1	Scope	**1**	Scope
2	Normative references	**2**	Normative references
3	Terms and definitions	**3**	Terms and definitions
4.1	Understanding the organization and its context	**8.3**	Preventive action
4.2	Understanding the needs and expectations of interested parties	**5.2.1(c)**	Identify and address legal and regulatory requirements and contractual security obligations
4.3	Determining the scope of the information security management system	**4.2.1 a)** **4.2.3 f)**	Define scope and boundaries Ensure the scope remains adequate
4.4	Information security management system	**4.1**	General requirements
5.1	Leadership and commitment	**5.1**	Management commitment
5.2	Policy	**4.2.1 b)**	Define an ISMS policy
5.3	Organizational roles, responsibilities and authorities	**5.1 c)**	Establishing roles and responsibilities for information security
6.1.1	Actions to address risks and opportunities - general	**8.3**	Preventive action
6.1.2	Information security risk assessment	**4.2.1 c)** **4.2.1 d)** **4.2.1 e)**	Define the risk assessment approach Identify the risks Analyse and evaluate the risks

Continued >>

Mapping tables – continued

ISO/IEC 27001:2013	ISO/IEC 27001:2005
6.1.3 Information security risk treatment	**4.2.1 f)** Identify and evaluate options for the treatment of risks **4.2.1 g)** Select control objectives and controls for the treatment of risks **4.2.1 h)** Obtain management approval of the proposed residual risks **4.2.1 j)** Prepare a Statement of Applicability **4.2.1 j)** Prepare a Statement of Applicability **4.2.2 a)** Formulate a risk treatment plan
6.2 Information security objectives and planning to achieve them	**5.1 b)** Ensuring that ISMS objectives and plans are established
7.1 Resources	**4.2.2 g)** Manage resources for the ISMS **5.2.1** Provision of resources
7.2 Competence	**5.2.2** Training, awareness and competence
7.3 Awareness	**4.2.2 e)** Implement training and awareness programmes **5.2.2** Training, awareness and competence
7.4 Communication	**4.2.4 c)** Communicate the actions and improvements **5.1 d)** Communicating to the organization
7.5 Documented information	**4.3** Documentation requirements
8.1 Operational planning and control	**4.2.2 f)** Manage operations of the ISMS
8.2 Information security risk assessment	**4.2.3 d)** Review risk assessments at planned intervals
8.3 Information security risk treatment	**4.2.2 b)** Implement the risk treatment plan **4.2.2 c)** Implement controls
9.1 Monitoring, measurement, analysis and evaluation	**4.2.2 d)** Define how to measure effectiveness **4.2.3 b)** Undertake regular reviews of the effectiveness of the ISMS **4.2.3 c)** Measure the effectiveness of controls
9.2 Internal Audit	**4.2.3 e)** Conduct internal ISMS audits **6** Internal ISMS audits
9.3 Management review	**4.2.3 f)** Undertake a management review of the ISMS **7** Management review of the ISMS
10.1 Nonconformity and corrective action	**4.2.4** Maintain and improve the ISMS **8.2** Corrective action
10.2 Continual improvement	**4.2.4** Maintain and improve the ISMS **8.1** Continual improvement

Table B lists the control groups in Annex A to ISO/IEC 27001:2013 in the left hand column. Each of these has a common control objective. The number in brackets refers to the number of controls in that group. On the right hand side there are eleven columns corresponding to the controls in each of the eleven major clause titles in Annex A to ISO/IEC 27001:2005. A cross means that there is a correspondence between the 2013 and 2005 controls. In order to see the exact relationships, please consult the detailed mapping data.

Table B: Mapping of Annex A controls

ISO/IEC 27001:2013 (number of controls)	ISO/IEC 27001:2005

	Security Policy A.5	Organization A.6	Asset management A.7	Human resources A.8	Physical A.9	Communications A.10	Access control A.11	Acquisition A.12	Incident A.13	Business continuity A.14	Compliance A.15
A.5.1 Management direction for information security (2)	X										
A.6.1 Internal organization (5)		X		X		X					
A.6.2 Mobile devices and teleworking (2)							X				
A.7.1 Prior to employment (2)				X							
A.7.2 During employment (3)				X							
A.7.3 Termination and change of employment (1)				X							
A.8.1 Responsibility for assets (4)			X	X							
A.8.2 Information classification (3)			X			X					
A.8.3 Media handling (3)						X					
A.9.1 Business requirements of access control (2)							X				
A.9.2 User access management (6)				X			X				
A.9.3 User responsibilities (1)							X				
A.9.4 System and application access control (5)							X	X			
A.10.1 Cryptographic controls (2)								X			
A.11.1 Secure areas (6)					X						
A.11.2 Equipment (9)					X		X				
A.12.1 Operational procedures and responsibilities (4)						X					
A.12.2 Protection from malware (1)						X					
A.12.3 Backup (1)						X					
A.12.4 Logging and monitoring (4)						X					
A.12.5 Control of operational software (1)								X			
A.12.6 Technical vulnerability management (2)								X			
A.12.7 Information systems audit considerations (1)											X
A.13.1 Network security management (3)						X	X				
A.13.2 Information transfer (4)		X				X					
A.14.1 Security requirements of information systems (3)						X		X			
A.14.2 Security in development and support processes (9)						X		X			
A.14.3 Test data (1)								X			
A.15.1 Information security in supplier relationships (3)		X									
A.15.2 Supplier service delivery management (2)						X					
A.16.1 Management of information security incidents and improvements (7)									X		
A.17.1 Information security continuity (3)										X	
A.17.2 Redundancies (1)											
A.18.1 Compliance with legal and contractual requirements (5)											X
A.18.2 Information security reviews (3)		X								X	

Transition guidance

Strategies

Transition strategy might be one of the following:

1. A straightforward "make-over", taking the minimum necessary changes to the existing ISMS processes and existing documentation; or
2. Take a completely fresh look at the ISMS, using the revised standard to make improvements, which might be quite significant for some organizations..

Transitioning using the minimalistic strategy might be accomplished quite quickly. Given the improvements of ISO/IEC 27001:2013 over its predecessor, organizations are encouraged to transition as soon as they can rather than put off their transition to the latest possible time. However, once detailed planning for transition is underway, organizations may wish to make improvements. Whilst this is encouraged, organizations need to decide whether to:

1. Highlight them as opportunities for improvement with the intention of making the changes at an appropriate time in the future; or
2. Make the changes immediately.

The first course of action is more typical of an organization that has adopted a minimalistic transition strategy, whilst the second is more likely if the organization is using the transition as a reason for making other changes.

Where to start

In both cases, a sensible place to start is with a gap analysis between the existing ISMS and the new version of the standard. This will then form the basis for the tasks required in the transition "project". Knowing how the existing ISMS conforms to the previous standard may also be of assistance, as it will help to identify areas with existing documented information that will require changing.

ISMS changes

Remember that the changes that you make to existing documented information should be recorded in order to comply with Clause 7.5.

Areas where changes may be minimal

Documented information

'Documented information' is a new term that applies to what the 2005 version of the standard referred to as 'documents' and 'records'. In transitioning to ISO/IEC 27001:2013, simply replace the terms 'documents' and 'records' with the term 'documented information'. If you need to make a distinction, recognize that documents are statements of intent whereas records are evidence of past performance.

Policy

There is a requirement in ISO/IEC 27001:2005 to produce an ISMS policy, which contains the information security policy and risk criteria. The policy requirements in ISO/IEC 27001:2013 (Clause 5.2) only refer to the information security policy, but there is a requirement (Clause 6.1.2) to establish and maintain the risk criteria, and later on in that clause a requirement to retain documented information about the risk assessment process. As an organization will have already documented its information security policy and risk criteria in its ISMS policy, and since ISO/IEC 27001:2013 does not give names to documents, an organization may decide to keep its ISMS policy the same. There is even no need to change its name. All an organisation needs is to know is which of the ISO/IEC 27001:2013 documented information requirements it meets.

However, there are other documented information requirements in ISO/IEC 27001:2013 that an organization may consider to be matters of policy, and therefore should be included in its 'ISMS' policy. These are:

1. The criteria for performing information security risk assessments (see Clause 6.1.2 a) 2));
2. The organization's policy towards releasing its information security policy to interested parties (see Clause 5.2 g)); and
3. The organization's policy regarding external communications (see Clause 7.4).

There are also two requirements that concern 'commitment', see Clauses 5.2 c) and d). Whilst policies can be written to demonstrate such commitment, organizations may wish to include two statements of intent, one for each of these requirements.

Risk assessment

In contrast to ISO/IEC 27001:2005, ISO/IEC 27001:2013 does not explicitly require the identification of assets, threats and vulnerabilities as a prerequisite to the identification of risks. It also uses the vocabulary of ISO 31000 (Risk management – principles and guidelines) and therefore ISO/IEC 27001:2013 refers to consequences rather than impacts. However, the general structure of the requirements (identify risks, assess consequences and likelihoods) is the same as ISO/IEC 27001:2005 and therefore a method that conforms to the requirements of ISO/IEC 27001:2005 should also conform to the requirements of ISO/IEC 27001:2013. This means that little or no change should be required to existing documented information relating to the risk assessment/risk treatment methodology or its implementation.

Control of documentation

No changes should be required to existing documented procedures concerning control of documentation.

Terms of reference for top management
A change may be required to accommodate the specific responsibilities given in Clauses 5.1 a) to h).

Responsibilities
A change may be required to accommodate the specific responsibilities given in Clauses 5.3 a) and b).

Awareness
A change may be required to accommodate the requirements of Clause 7.4 as the process of creating awareness may be regarded as a form of communication.

Internal audit
No changes should be required to existing documented procedures relating to internal audit.

Management review
No changes should be required to existing documented management review procedures, apart from ensuring that the topics listed in Clauses 9.3.a) – f) are considered.

Corrective action
Existing procedures may need to be strengthened to ensure you react to nonconformities and take action, as applicable, to control and correct them and deal with the consequences. You may also be required to determine whether similar nonconformities exist, or could potentially occur, and ensure that the appropriate corrective actions are implemented to deal with the effects.

Improvement
Ensure that existing procedures for continual improvement are extended to cover the suitability and adequacy of the ISMS as well as its effectiveness.

Areas that potentially require a rethink

Scope of the management system
The wording of Clause 4.3 (and in particular 4.3 c)) is intended to make it clear that the scope of the ISMS (as distinct from the scope of certification) includes everything that is of interest to the ISMS. Therefore the scope will include external risk sources, such as hackers and natural disasters, as well as any functions that are outsourced.

If, on reflection, an organization considers that there are entities that should be included within the scope of its ISMS that were previously excluded, the transition to ISO/IEC 27001:2013 I provides an opportunity to redefine the ISMS scope, as well as demonstrate conformance with Clause 4.3.

Information security objectives
If an organization considers its information security objectives as being timeless policy objectives, the requirement of Clause 6.2, which refers to 'relevant functions and levels', may come as a shock. However, it may only require a change to the way conformance is described. It is likely that an organization already sets objectives at all relevant functions and levels, and it is only a question of recognizing that it does this and describing how.

For example, it is good practice when placing actions to define objectives, assign responsibilities and set targets dates for completion. If an organization already does this, then it already conforms to this clause.

Areas requiring updating

The Statement of Applicability
Annex A has been updated to reflect the controls that are now described in ISO/IEC 27002:2013. Whilst organizations are no longer required to select controls from Annex A, it is still used to determine whether any necessary controls have been omitted (see Clause 6.1.3 c)) and organizations are required to produce a SOA. The format of an ISO/IEC 27002:2013 conformant SOA doesn't need to be different from the previous standard. However, the control set is different, and therefore organizations will be required to update their SOAs. When doing so, be careful to ensure that control implementation strictly conforms to the wording given in Annex A.

New requirements that may be satisfied already

Interested parties and their requirements
Clause 4.2 requires an organization to determine the interested parties that are relevant to the ISMS, and their requirements. It is likely that an organization already knows this information. For example, interested parties may include customers and suppliers, and their requirements will be documented in contracts, purchase orders and specifications, etc. Therefore all that needs to be done is identify where this information is documented and reference it. The organization is also likely to already make use of this information, providing conformance with other clauses such as 6.1.

Integration
Clause 5.1 b) requires top management to ensure integration of the ISMS requirements into the organization's business processes. If the business functions of an organization were to be represented by a set of one or more workflow diagrams and therefore the activities that correspond to the ISMS requirements are spread throughout these work flows, then the integration requirement is probably met. However if the ISMS requirements are contained in a single workflow which contains nothing else, then the integration requirement is probably not met.

In the first case, it is then a question of how best to demonstrate conformance. If workflow diagrams exist, or can be visualized, e.g. through a software interface, then that would be an easy way to demonstrate conformance. If the integration requirement is not met, then the workflow concept may provide a route to achieving conformance.

Communication
The requirements of Clause 7.4 (communications) are more specific than the equivalent requirements in the previous version of the standard. Nevertheless, the new requirements follow common practice and therefore the communication requirements may already be satisfied.

New requirements that may present a challenge

Issues

It is likely that the issues referred to in Clause 4.1 would be well known to an organization, but not necessarily written down; certainly not in a way which would demonstrate conformance.

An important issue for most organizations would be its motivation for having an ISMS. An organization would know what that was and it would have been a major driver in how the original ISMS had been designed. Note that this motivation may have changed over time: the original motivation being superseded by another as the benefits of having the ISMS management system had been realized.

Another important issue would be those concerned with information security. If these are unknown or the organization is uncertain of them, it may be possible to reverse engineer them from a consideration of the information security policy, objectives and the information security risk assessment and risk treatment.

Other issues, which are likely to have been already addressed by an organization would relate to the operation of the ISMS, such as management commitment and staff motivation. Finally, organizations should consider looking through management meeting minutes and its records of preventive actions for further issues. After all, Clauses 4.1 and 6.1.1 are the new way to deal with preventive action.

Actions to address risks and opportunities – general

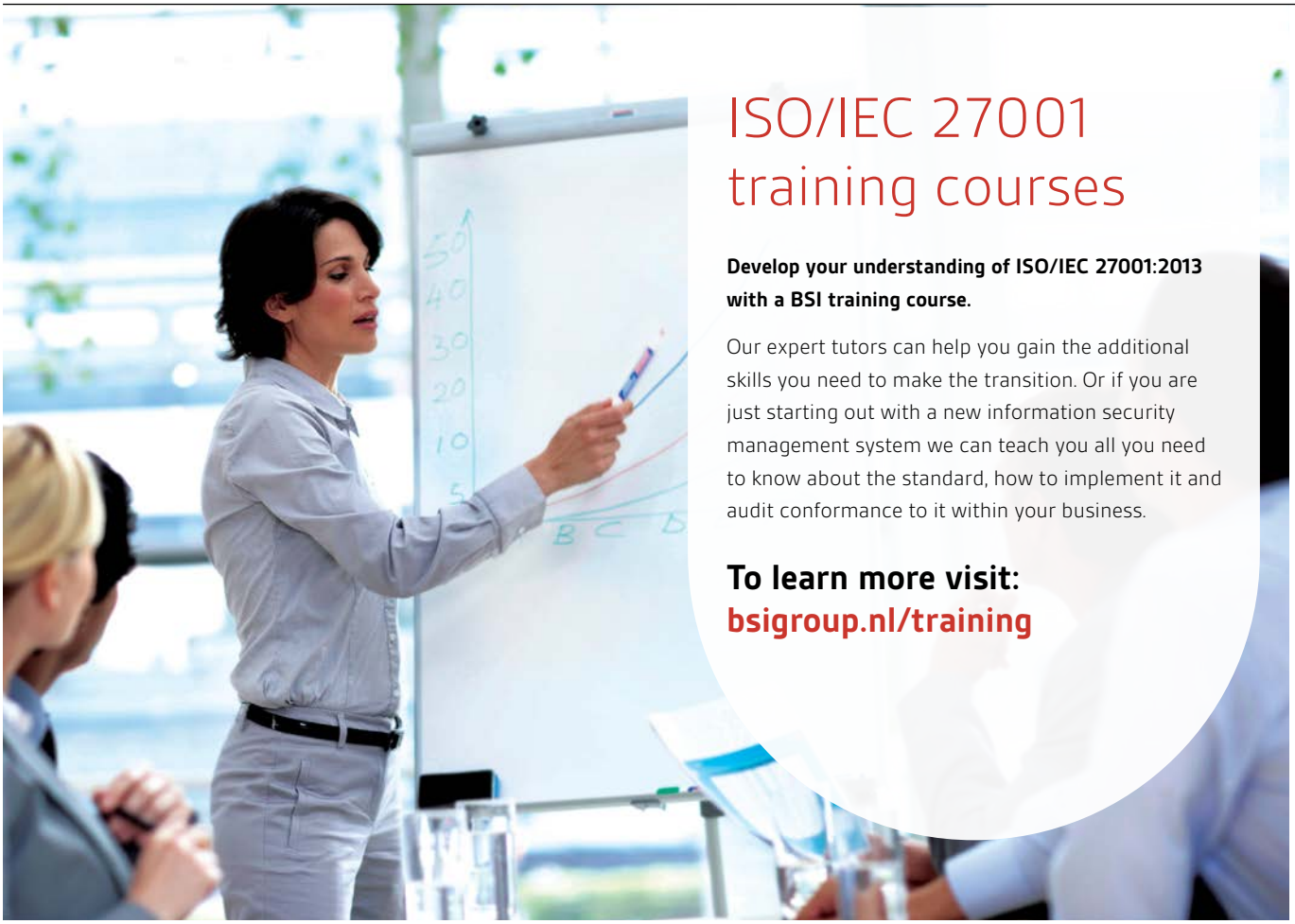
Existing preventive action procedures will need to be revised or replaced to ensure conformance with Clauses 4.1, 4.2 and 6.1.1. Organizations are directed towards information given earlier in this brochure.

Monitoring, measurement, analysis and evaluation

The requirements of Clause 9.1 are more detailed and exact than the requirements for the ISMS and control effectiveness in ISO/IEC 27001:2005. From the perspective of transition it may be best to start with a clean sheet of paper. Organizations are directed towards the information given earlier in this brochure.

Concluding remarks

All organizations are different and this guidance needs to be interpreted in the context of the individual needs of each organization. What may turn out to be easy for some may be challenging for others and vice versa. It is hoped that this guidance will be a useful starting position for most organizations.

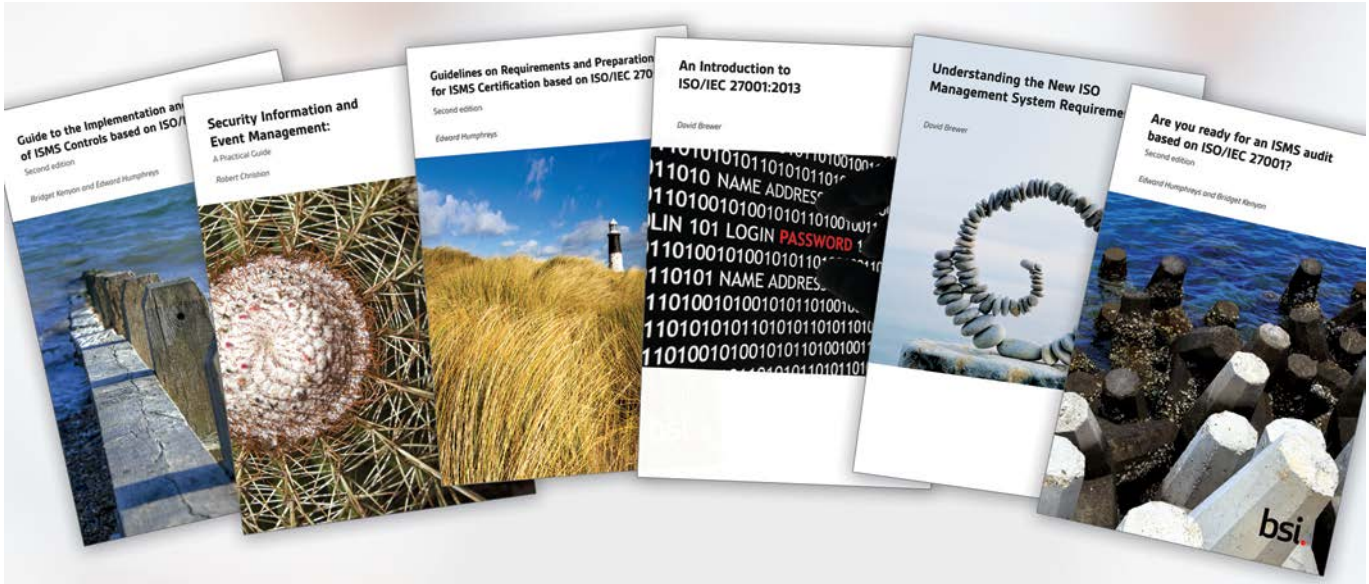


ISO/IEC 27001 training courses

Develop your understanding of ISO/IEC 27001:2013 with a BSI training course.

Our expert tutors can help you gain the additional skills you need to make the transition. Or if you are just starting out with a new information security management system we can teach you all you need to know about the standard, how to implement it and audit conformance to it within your business.

To learn more visit:
bsigroup.nl/training



New information security books now available

Do you need additional information to help you make the transition?

Whether you are new to the standard, just starting the certification process, or already well on your way, our books will give you a detailed understanding of the new standards, guidelines on implementation, and details on certification and audits – all written by leading information security specialists, including David Brewer, Bridget Kenyon, Edward Humphreys and Robert Christian.

Sample chapters are available

Find out more www.bsigroup.nl

David Brewer – biography

David Brewer, PhD, FBCS is recognized worldwide for the contributions he has made to information security management. He was one of the first consultants to advise the British Government on information security matters in the early 1980s and was one of the developers of the original ISMS standard, BS 7799-2:2002. He has provided ISMS training and consultancy in Europe, the US, East Africa, the Middle East and the Far East, and he is the administrator of an integrated management system conforming to ISO 9001, ISO/IEC 27001 and ISO 22301. He is an member of the ISO committee responsible for the ISO/IEC 27000 series of standards, played a significant role in developing ISO/IEC 27001:2013 and is a co-editor for the revision of ISO/IEC 27004.

We know ISO/IEC 27001; BSI shaped the original standard.

BSI...

- Shaped the original ISO/IEC 27001 standard
- Has the most highly trained and knowledgeable assessors
- Offers the widest range of support solutions in the market place
- Is the number one certification body in the UK, USA and Korea
- Looks after more than 70,000 global clients
- Has an unrivalled International reputation for excellence

bsi.

BSI Group
Adam Smith Building
Thomas R. Malthusstraat 3c
1066 JR Amsterdam
The Netherlands

T: +31 (0)20 346 0780
E: info.nl@bsigroup.com
bsigroup.nl