INTERNATIONAL STANDARD

ISO/IEC 27013

Second edition
2015-12-01

Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Technologies de l'information — Techniques de sécurité — Guide sur la mise en oeuvre intégrée d'ISO/IEC 27001 et ISO/IEC 20000-1

Reference number
ISO/IEC 27013:2015(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 27013:2012), which has been technically revised.

Introduction

The relationship between information security management and service management is so close that many organizations already recognise the benefits of adopting the two International Standards for these domains: ISO/IEC 27001 for information security management and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to achieve conformity with the requirements specified in one of these International Standards and then make further improvements to achieve conformity with the requirements of the other.

There are a number of advantages in implementing an integrated management system that takes into account not only the services provided but also the protection of information. These benefits can be experienced whether one International Standard is implemented before the other, or both International Standards are implemented simultaneously. Management and organizational processes, in particular, can derive benefit from the mutually reinforcing concepts and similarities between these International Standards and their common objectives.

Key benefits of an integrated implementation of information security management and service management include the following:

a) the credibility, to internal or external customers of the organization, of an effective and secure service;

b) the lower cost of an integrated programme of two projects, where effective and efficient management of both services and information security are part of an organization's strategy;

c) a reduction in implementation time due to the integrated development of processes common to both standards;

d) better communication, reduced cost and improved operational efficiency through elimination of unnecessary duplication;

e) a greater understanding by service management and security personnel of each others' viewpoints;

f) an organization certified for ISO/IEC 27001 can more easily fulfil the requirements for information security specified in ISO/IEC 20000-1:2011, 6.6, as both International Standards are complementary in requirements.

The guidance in this International Standard is based upon the published versions of both ISO/IEC 27001 and ISO/IEC 20000-1.

This International Standard is intended for use by persons with knowledge of both, either or neither of the International Standards ISO/IEC 27001 and ISO/IEC 20000-1.

It is expected that all readers have access to copies of both ISO/IEC 27001 and ISO/IEC 20000-1. Consequently, this International Standard does not reproduce parts of either of those International Standards. Equally, it does not describe all parts of each International Standard comprehensively. Only those parts where subject matter overlaps are described in detail.

This International Standard does not provide guidance associated with the various legislation and regulations outside the control of the organization. These can vary by country and impact the planning of an organization's management system.

Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

1 Scope

This International Standard provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organizations that are intending to either

a) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa,

b) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together, or

c) integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1.

This International Standard focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.

In practice, ISO/IEC 27001 and ISO/IEC 20000-1 can also be integrated with other management system standards, such as ISO 9001 and ISO 14001.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20000-1:2011, *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC/TR 20000-10, *Information technology — Service management — Part 10: Concepts and terminology*

ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 27000, ISO/IEC 20000-1 and ISO/IEC/TR 20000-10 apply.

The following abbreviations apply.

ISMS information security management system (from ISO/IEC 27001)

SMS service management system (from ISO/IEC 20000-1)

Annex A provides a comparison of content at a clause level between ISO/IEC 27001 and ISO/IEC 20000-1.

Annex B provides a comparison of terms defined in the following:

— ISO/IEC 27000, the glossary for ISO/IEC 27001;

— terms used in ISO/IEC 27001;

— terms defined or used in ISO/IEC 20000-1 or ISO/IEC/TR 20000-10.

4 Overviews of ISO/IEC 27001 and ISO/IEC 20000-1

4.1 Understanding the International Standards

An organization should have a good understanding of the characteristics, similarities and differences of ISO/IEC 27001 and ISO/IEC 20000-1 before planning an integrated management system for information security management and service management. This maximizes the time and resources available for implementation. 4.2 to 4.4 provide an introduction to the main concepts underlying both Internatonal Standards but should not be used as a substitute for a detailed review.

4.2 ISO/IEC 27001 concepts

ISO/IEC 27001 provides a model for establishing, implementing, maintaining and continually improving an ISMS to protect information. Information can take any shape, be stored in any form and be used for any purpose by, or within, the organization.

To achieve conformity with the requirements specified in ISO/IEC 27001, an organization should implement an ISMS based on a risk assessment process to identify risks to information. As part of this work, the organization should select, implement, monitor and review a variety of measures to manage these risks. These measures are known as controls. The organization should determine acceptable levels of risk, taking into account the requirements of interested parties relevant to information security. Examples of requirements are business requirements, legal and regulatory requirements or contractual obligations.

ISO/IEC 27001 can be used by any type and size of organization.

4.3 ISO/IEC 20000-1 concepts

ISO/IEC 20000-1 can be used by organizations, or parts of organizations, which use or provide services. This adds value for both the customer and the service provider. All processes covered by the standard should be controlled by the service provider, even if some processes are operated by other parties. It is only the service provider that can achieve conformity with the requirements specified in ISO/IEC 20000-1.

The SMS directs and controls a service provider's activities and resources in the design, development, transition, operation and improvement of services to fulfil service requirements as agreed with its customer(s).

To fulfil the requirements specified in ISO/IEC 20000-1, the service provider should implement a range of specific service management processes. These include incident management, change management and problem management, amongst others. Information security management is one of the ISO/IEC 20000-1 service management processes.

ISO/IEC 20000-1 can be used by any type and size of organization.

4.4 Similarities and differences

Service management and information security management are often treated as if they are neither connected nor interdependent. The context for such separation is that service management can easily be related to efficiency and profitability, while information security management is often not understood to be fundamental to effective service delivery. As a result, service management is frequently implemented first. However, as shown in Figure 1, many control objectives and controls in ISO/IEC 27001:2013, Annex A are also included within the service management requirements for an SMS specified in ISO/IEC 20000-1.

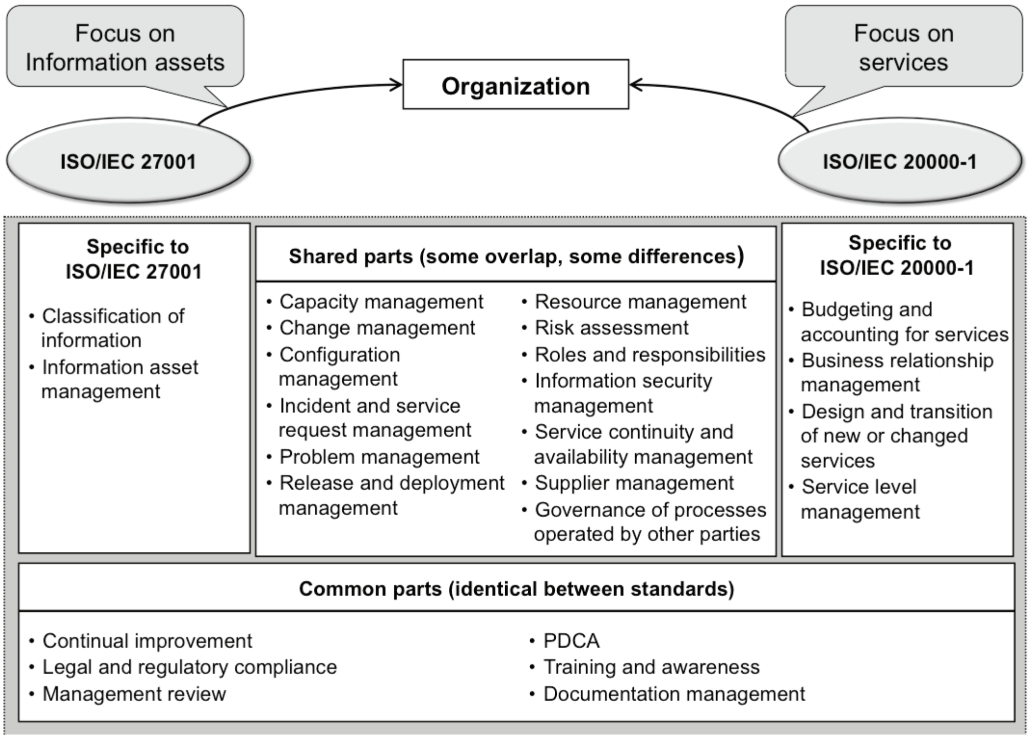

Figure 1 — Comparison between concepts in ISO/IEC 27001 and ISO/IEC 20000-1

Information security management and service management clearly address very similar processes and activities, even though each management system highlights different details. See Annex A for further information. When working with the two standards, it should be understood that their characteristics differ in more than one respect. For example, their scopes differ (see 5.2). They also have different goals. ISO/IEC 20000-1 is designed to ensure that the organization provides effective services, while ISO/IEC 27001 is designed to enable the organization to manage information security risk and prevent security incidents.

5 Approaches for integrated implementation

5.1 General

An organization planning to implement both ISO/IEC 27001 and ISO/IEC 20000-1 can be in one of three states as follows:

— ad-hoc management arrangements exist which cover both information security management and service management (formal management systems can also exist for other areas, such as quality management);

— there is a management system based upon one of these two International Standards;

— there are separate management systems based on the two International Standards but these are not integrated.

An organization planning to implement an integrated management system for information security and service management should consider at least the following:

a) other management system(s) already in use (e.g. a quality management system);

b) all services, processes and their interdependencies in the context of the integrated management system;

c) elements of each standard which can be merged and how they can be merged;

d) elements that are to remain separate;

e) the impact of the integrated management system on customers, suppliers and other parties;

f) the impact on technology in use;

g) the impact on, or risk to, services and service management;

h) the impact on, or risk to, information security and information security management;

i) education and training in the integrated management system;

j) phases and sequence of implementation activities.

5.2 Considerations of scope

One area where the two International Standards differ significantly is on the subject of scope, namely, what assets, processes and parts of the organization the management system should include.

ISO/IEC 20000-1 is concerned with the design, transition, delivery and improvement of services to deliver business value. This is achieved through defining the service requirements to deliver objectives and then coordinating the policies, processes, plans and resources to develop, manage and improve those services. The scope of ISO/IEC 20000-1 includes the objectives, policies, plans, processes and resources as well as the services.

ISO/IEC 27001 is concerned with how to manage information security risk. The scope of ISO/IEC 27001 covers those parts of its activities that the organization wishes to secure. In this sense, the scopes of the two International Standards are described differently. As a result, it is possible to implement ISO/IEC 27001 for the same scope as ISO/IEC 20000-1, but ISO/IEC 20000-1 cannot be applied to the whole organization unless the organization is wholly a service provider.

Thus, certain processes, assets and roles in the organization may be excluded from the scope for an ISMS developed to achieve conformity with the requirements in ISO/IEC 27001. For ISO/IEC 20000-1, these may not be excluded from scope if they are part of, or contribute to, the services in the scope of the SMS. The ISMS scope may also be defined exclusively by a clear physical boundary, such as a security perimeter.

In some cases, the full requirements of the two International Standards cannot be implemented for all, or even part, of the organization's activities. This can be the case if, for example, an organization cannot conform to the requirements specified in ISO/IEC 20000-1 because it does not have governance of all processes operated by other parties.

An organization can implement an SMS and an ISMS with some overlap between the different scopes. Where activities lie within the scope of both ISO/IEC 27001 and ISO/IEC 20000-1, the integrated management system should take both International Standards into account (see Annex A). Differences in scope can result in some services included in the SMS being excluded in the ISMS. Equally, the SMS can exclude processes and functions of the ISMS. For example, some organizations choose to implement an ISMS only in their operation and communication functions, while application management services are included in their SMS. Alternatively, the ISMS can cover all the services, while the SMS can cover only the services for a particular customer or some services for all customers. The organization should align the scopes of the management systems as much as possible to ensure successful integration.

NOTE Guidance on scope definition for ISO/IEC 20000-1 is available in ISO/IEC 20000-3. Guidance on the scope definition for ISO/IEC 27001 is available in ISO/IEC 27003.

5.3 Pre-implementation scenarios

5.3.1 General

An organization planning an integrated management system can be in one of three states, as described in 5.3.2 to 5.3.4. In all cases, the organization has some form of management processes or it would not exist. The following clauses provide suggestions for implementation in each of the three states also described in 5.1.

5.3.2 Neither standard is currently used as the basis for a management system

It is easy to assume that, where neither standard is implemented, there are no policies, processes and procedures and that therefore the situation is simple to deal with. However, this is a misconception.

All organizations will have some form of management system. This should be adapted to achieve conformity with the requirements specified in either or both of the standards.

The decision regarding the order in which the two management systems will be implemented should be based on business needs and priorities. Decisions can be influenced by whether the primary driver is competitive positioning or the need to demonstrate compliance to a customer.

Another important decision is whether to implement both standards concurrently or sequentially. If the implementation is sequential, one standard is implemented and then the scope is extended to include the additional requirements of the other. See 5.3.3. Both the ISMS and the SMS can be implemented concurrently, if implementation activities and efforts can be coordinated and duplication minimised. However, depending upon the nature of the organization, it can be prudent to start with one standard and then expand the scope to include the other.

These considerations are illustrated in the following scenarios.

a) An organization that provides services should start with the implementation of ISO/IEC 20000-1 and then, working from lessons learned during that implementation, expand the management system to include ISO/IEC 27001.

b) An organization that is using suppliers, including other parties, for delivery of some parts of the service should initially focus on ISO/IEC 20000-1. ISO/IEC 20000-1 includes more requirements for managing other parties, including suppliers. This allows resolution of supplier management and process control issues. The organization should then proceed to ISO/IEC 27001.

c) A small organization should focus on one of either ISO/IEC 27001 or ISO/IEC 20000-1, depending on its level of reliance upon service management or information security.

d) A large organization with internal service delivery should handle the implementation as a single project. If this is not possible, then it should divide the implementation into two parallel sub-projects within one overarching programme of work. Each sub-project should manage one standard and integrate the implementations as a mutual sub-project. If this approach is chosen, it is vital to ensure that the implementations are compatible as they are developed. This can introduce additional overhead and further risk to the outcome, so should only be used if there is no alternative.

e) Any organization that places a high level of importance on information security should first implement an ISMS which conforms to the requirements specified in ISO/IEC 27001. The next stage should be the expansion of that management system to fulfil the requirements specified in ISO/IEC 20000-1, supporting information security.

An integration working group holding regular meetings during the implementation of both management systems can help in ensuring the two are aligned.

5.3.3 A management system exists which fulfils the requirement of one of the standards

Where a management system has already achieved conformity with the requirements specified in one of the two standards, the primary goal should be to integrate the requirements of the other standard. This should be done without suffering any loss of service or jeopardising information security of the service. However, the existing management system should be broken down into its individual elements. This should be carefully planned in advance, with existing documentation being reviewed by experts in the standard that is being introduced, and by experts in the standard already implemented.

The organization should identify the attributes of the established management system, including at least the following:

a) scope;

b) organizational structure;

c) policies;

d) planning activities;

e) authorities and responsibilities;

f) practices;

g) risk management methodologies;

h) relevant processes;

i) procedures;

j) terms and definitions;

k) resources.

These attributes should then be reviewed to establish how they can be applied to the integrated management system. If a two-step approach is used, with one management system in place as step one, the second step is to implement the other management system. The scope for the second step should be defined and agreed before starting any implementation activities.

5.3.4 Separate management systems exist which fulfil the requirements of each standard

This last case is perhaps the most complex. It illustrates the issue of scope; see 5.2. It is possible that an organization has implemented an ISMS in one organizational area and has implemented an SMS in another. The organization can then decide to apply one or other of the standards across a wider scope of activities. At some point in time, the management systems will be implemented for the same activities. Alternatively, two organizations can be planning to merge. One has demonstrated conformity to the requirements specified in ISO/IEC 27001, while the other has demonstrated conformity to the requirements specified in ISO/IEC 20000-1.

A review should form the starting point, aiming to achieve the following:

a) identify and document the existing and proposed scopes to which each standard applies, paying particular attention to their differences;

b) compare the existing management systems and establish if there are any mutually incompatible aspects;

c) develop a business case to clarify the benefits of an integrated management system;

d) start to engage the stakeholders of both management systems with one another;

e) plan the best approach to achieving an integrated management system:

   1) start with a very broad outline view;

   2) review this at various levels in the organization to add details;

   3) provide feedback and suggested solutions to the appropriate level of authority to allow decisions to be taken.

Although there are many ways of integrating management systems whilst maintaining conformity, an extensive planning phase should be completed.

6 Integrated implementation considerations

6.1 General

In all cases, the organization's goal should be to produce a viable integrated management system that enables conformity with the requirements specified in both standards. The goal is not to compare the standards or to determine which is best or right. Where there is conflict between viewpoints, this should be resolved in a way which satisfies the requirements specified in both standards and ensures that the organization achieves continual improvement of its ISMS and SMS. The ideal integrated management system should be based on the most efficient approach from both standards, applied appropriately. This is also supported by use of additional details in one standard to supplement the other. Care should be taken to retain everything necessary for conformity to both standards.

Documented traceability should be maintained between the integrated management system and the requirements of each separate standard. To reduce effort, a single set of documentation can be created for the integrated management system. To support this, the organization can create traceability documentation such as a traceability matrix. This explicitly shows how the integrated management system conforms to the requirements of each of the standards. The benefits of this approach include being able to more easily demonstrate conformity in audits and reviews. These benefits also include being able to track which activities are necessary to demonstrate conformity to each standard.

6.2 Potential challenges

6.2.1 The usage and meaning of asset

In this Clause, the differences and similarities of usage and meaning of asset in ISO/IEC 27001 and ISO/IEC 20000-1 are discussed. Suggestions are given on how to reconcile the two standards.

In ISO/IEC 20000-1, an asset is different to an asset in ISO/IEC 27001. Asset is not a defined term in ISO/IEC 20000-1 or ISO/IEC 27001, so it is used in its normal English language sense of something of value. In some clauses in ISO/IEC 20000-1, the use of assets is linked to financial assets, such as software licences. In other clauses, assets are referred to as information assets. In contrast, ISO/IEC 27001 is based upon the concept of protecting information. ISO/IEC 27001:2013, Annex A includes asset management as a control. The word asset is used in ISO/IEC 20000-1 in the normal English sense: anything that is considered valuable or useful, such as a skill, quality, or person, etc. ISO/IEC 20000-1 also uses a defined term, configuration item (CI), as an element that needs to be controlled in order to deliver a service or services. The organization should therefore define what a CI is for its own purposes, taking into account its needs for efficiency. Information can be included in this definition. In ISO/IEC 20000-1, the configuration management database (CMDB) is the data store of all CIs and their interrelations. Some organizational assets will not be in the CMDB (e.g. PCs not used to deliver or access the service). Equally, some CIs might not be considered to be assets under ISO/IEC 20000-1, e.g. people. Assets in ISO/IEC 20000-1 normally have monetary value.

In ISO/IEC 27001, the focus is on information security risk assessment and risk treatment, which is applied to all information within scope of the ISMS. The form of information is irrelevant: it can be paper, electronic, etc. As a result, information, or the resources used for handling information, can be