INTERNATIONAL STANDARD

ISO/IEC 27013

First edition
2012-10-15

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/CEI 27001 et ISO/CEI 20000-1

Reference number
ISO/IEC 27013:2012(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Figures

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 27013 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in co-operation with Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

Introduction

The relationship between information security and service management is so close that many organizations already recognize the benefits of adopting both standards: ISO/IEC 27001 for information security, and ISO/IEC 20000-1 for service management. It is common for an organization to improve the way it operates to conform with the requirements of one International Standard and then make further improvements to conform to the requirements of the other.

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

Key benefits of an integrated implementation include:

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 achieving both service management 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) 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 in ISO/IEC 20000-1:2011, subclause 6.6, as both International Standards are complementary in requirements.

The guidance is based upon the published versions of both International Standards, ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011.

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 International Standards. Consequently, this International Standard does not reproduce parts of either standard. 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 give 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 which 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;

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

This International Standard focuses exclusively on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.

In practice, ISO/IEC 27001 and ISO/IEC 20000-1 can also be integrated with other management systems, 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 — Service management system requirements*

ISO/IEC 27000:2009, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms, abbreviated terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2009 and ISO/IEC 20000-1:2011 apply.

For the purposes of this document, the following abbreviations apply.

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

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

Annex A of this International Standard provides a comparison of content at a clause level between ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011.

Annex B of this International Standard provides a comparison of terms defined in:

- ISO/IEC 27000:2009, the glossary for ISO/IEC 27001:2005;
- terms used in ISO/IEC 27001;
- terms defined or used in ISO/IEC 20000-1:2011.

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. This maximises the time and resources available for implementation. Clauses 4.2 to 4.4 of this International Standard provide an introduction to the main concepts underlying both 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, operating, monitoring, reviewing, maintaining and improving an ISMS to protect information assets. Information assets encompass information in any shape, stored in any form, and used for any purpose by, or within, the organization.

To achieve conformity with ISO/IEC 27001, an organization should implement an ISMS based on a risk assessment process to identify risks to information assets. 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 business requirements and externally imposed requirements. Examples of externally imposed requirements are statutory 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. However, all processes covered by the standard are controlled by the service provider, and it is only the service provider that can achieve conformity with ISO/IEC 20000-1. The standard is primarily concerned with ensuring that services fulfil service requirements and provide value for both the customer and the service provider.

Service management directs and controls a service provider's activities and resources in the design, development, transition, delivery and improvement of services to fulfil service requirements as agreed with their customer(s).

To fulfil the requirements of the standard, a range of specific service management processes should be implemented by the service provider. 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 27001:2005, Annex A, are also included, within the service management requirements in ISO/IEC 20000-1.

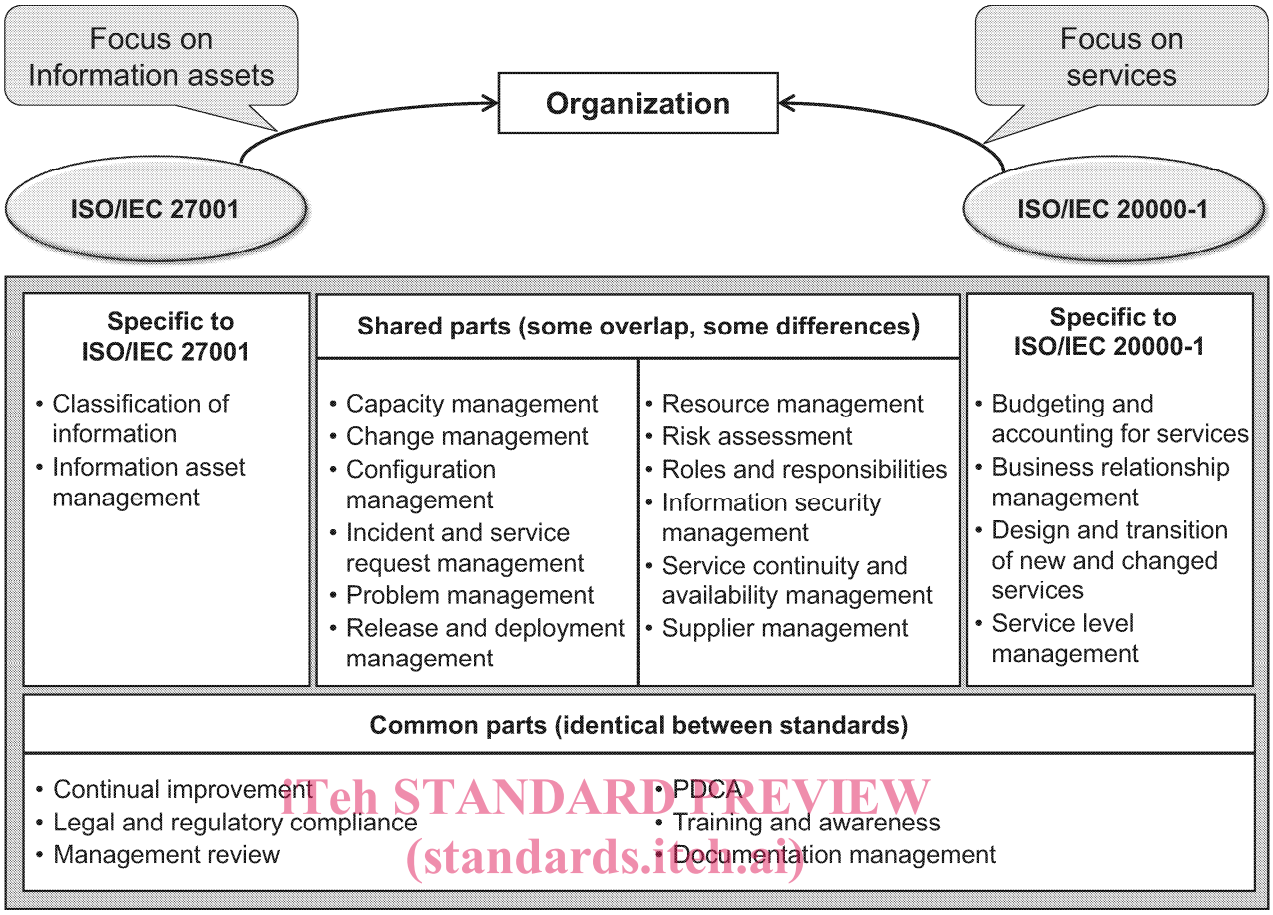

Figure 1 — Comparison between concepts in ISO/IEC 27001 and ISO/IEC 20000-1

Information security management and service management clearly address very similar processes and activities, even though one management system highlights some details more than others. See Annex A of this International Standard for further information. When working with the two standards, it should be understood that they have different characteristics in more than one respect. For example, their scopes differ, see Clause 5.2 of this International Standard. 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:

- 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 standard;
- there are separate management systems based on the two standards, but these are not integrated.

An organization planning to implement an integrated management system 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) impact of the integrated management system on customers, suppliers and other parties;

f) impact on technology in use;

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

h) 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 requirements for design, transition, delivery and improvement of services to fulfil requirements. This is done through a set of processes. Therefore, the scope of ISO/IEC 20000-1 comprises the management processes within the organization, and the services provided. ISO/IEC 27001 is concerned with how to manage information security risk. The scope of ISO/IEC 27001 covers those parts of its activities which the organization wishes to secure. In this sense, the scopes of the two 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 meet ISO/IEC 27001. For ISO/IEC 20000-1, these may not be excluded from scope if they are part of, or contribute to, the service 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 two International Standards cannot be implemented for all, or even part, of the organization's activities. For example, if an organization cannot conform to the requirements of 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 standards into account, see Annex A of this International Standard. 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 standards as much as possible to ensure that the management systems can be successfully integrated.

NOTE Guidance on scope definition for ISO/IEC 20000-1 is available in ISO/IEC 20000-3:2012, Guidance on scope definition and applicability of ISO/IEC 20000-1.

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 Clauses 5.3.2 to 5.3.4 of this International Standard. 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 Clause 5.1 of this International Standard.

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 therefore the situation is simple to deal with. Unfortunately, this is a misconception. Organizations which do not have a management system based upon either ISO/IEC 27001 or ISO/IEC 20000-1 are likely to have some form of management system. This will then have to be adapted to achieve conformity with 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. Decisions can be influenced by whether the incentive is competitive positioning using one or other standard, or a need to demonstrate the requirements of one or other standard for an existing customer or a new customer.

Another important decision is whether to implement a management system based on both standards from the start, or whether to implement a management system based upon one standard then extend it to include requirements of the other, see Clause 5.3.3 of this International Standard. Both standards can be implemented simultaneously, if implementation activities and efforts can be coordinated and duplication minimized. However, depending upon the nature of the organization, it can be prudent to start with one standard and then to implement the other.

These considerations are illustrated in the following scenarios.

a) An organization which 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 which is using suppliers, including other parties, for delivery of some parts of the service should initially focus on ISO/IEC 20000-1. This provides more requirements for other parties, including supplier management. 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 follow-on 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 which places a high level of importance on information security should first implement an ISMS which conforms to the requirements of ISO/IEC 27001. The next stage should be the expansion of that management system to meet the requirements of ISO/IEC 20000-1, supporting information security.

An integration working group / regular meetings during the implementation of both standards would 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 is already compliant with 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 which 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) 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 the other management system being implemented. The scope for each step should be defined and agreed before starting any implementation work.

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 Clause 5.2 of this International Standard. It is possible that an organization has implemented ISO/IEC 27001 in one organizational area, and has implemented ISO/IEC 20000-1 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 ISO/IEC 27001, while the other has demonstrated conformity to 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) start to engage the stakeholders in both management systems with one another;

d) plan the best approach to 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 which enables conformity with 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 of 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 ISO/IEC 20000-1, an asset is different to an information asset in ISO/IEC 27001. Asset is not a defined term in ISO/IEC 20000-1, so it is used in its normal English language sense of something of value. In some clauses in ISO/IEC 20000-1:2011 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 and has a formal definition for information asset. In the remainder of Clause 6.2 of this International Standard, the differences and similarities of usage and meaning in the two standards are discussed. Suggestions as to how to reconcile the two standards are included.

ISO/IEC 20000-1 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 asset” 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 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.

For ISO/IEC 27001, information assets are defined as knowledge or data that has value to the organization, regardless of their form, e.g. paper, electronic, etc. As a result, information assets can be CIs, but CIs are not necessarily information assets. For example, a data cable can be a CI, but is usually not an information asset. Figure 2 provides an illustration of the relationship between CIs and information assets. For an integrated management system, an information asset in ISO/IEC 27001 can be used by, or be part of, a service in ISO/IEC 20000-1.