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.

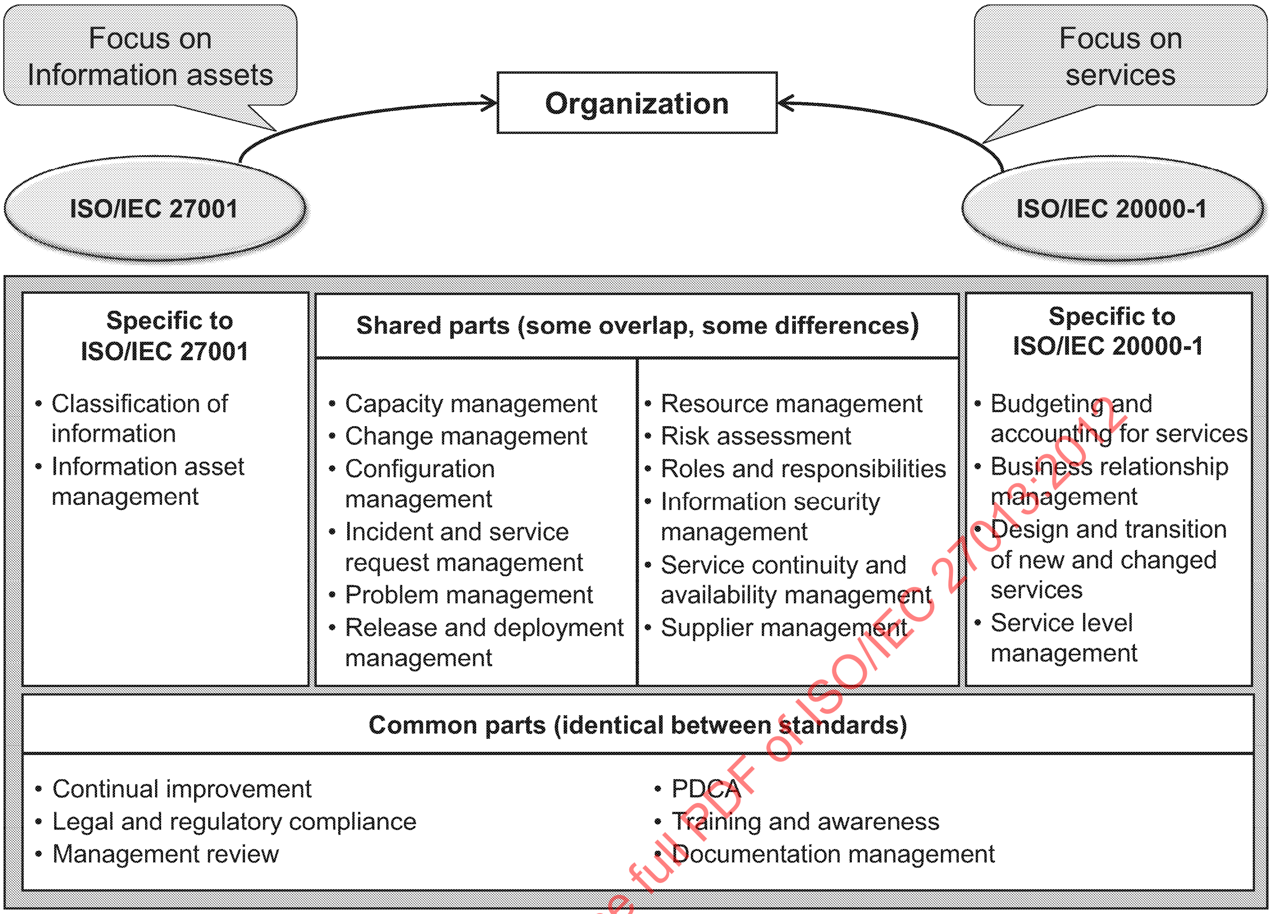
Focus on Information assets
Organization
Focus on services
ISO/IEC 27001
ISO/IEC 20000-1
Specific to ISO/IEC 27001
• Classification of information
• Information asset management
Shared parts (some overlap, some differences)
• Capacity management
• Change management
• Configuration management
• Incident and service request management
• Problem management
• Release and deployment management
• Resource management
• Risk assessment
• Roles and responsibilities
• Information security management
• Service continuity and availability management
• Supplier management
Specific to ISO/IEC 20000-1
• Budgeting and accounting for services
• Business relationship management
• Design and transition of new and changed services
• Service level management
Common parts (identical between standards)
• Continual improvement
• Legal and regulatory compliance
• Management review
• PDCA
• Training and awareness
• Documentation management

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.

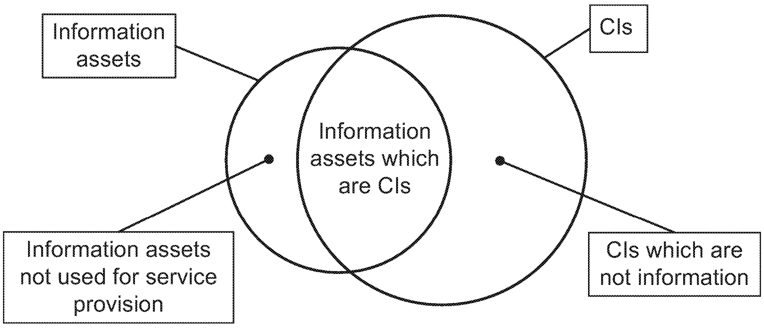
Information assets
CIs
Information assets which are CIs
Information assets not used for service provision
CIs which are not information

Figure 2 — Relationship between information assets in ISO/IEC 27001 and CIs in ISO/IEC 20000-1

Neither of the standards requires every CI or information asset to be listed individually. They can be grouped into types, such as hardware, or documents. As part of this process, their descriptions should be made as consistent as possible, simplifying conformity with both standards. For example, at the beginning of any integration work, a decision should be made on the way in which assets will be categorized and identified. This is to ensure unambiguous references can be made to assets. If the term information asset is used in the ISO/IEC 27001 sense, specific assets should be given an additional label to ensure that their status is recognised as CIs or financial assets in ISO/IEC 20000-1, see Annex B of this International Standard.

6.2.2 Design and transition of services

ISO/IEC 20000-1:2011, Clause 5 includes requirements for the design and transition of new or changed services. There is no directly equivalent clause in ISO/IEC 27001, although several aspects of service design, transition and delivery are covered in ISO/IEC 27001:2005, Annex A. However, an integrated management system should ensure that information security is considered in detail during the planning stages of the design and transition of new or changed services. Topics that should be considered include an assessment of the impact of the new or changed service on both the service and existing information security controls, see ISO/IEC 20000-1:2011, Clause 6.6.2. This should also be done for the closure of a service.

Planning of all new or changed services should include consideration of information security implications. This should be done regardless of whether the service falls within the scope of the ISMS.

6.2.3 Risk assessment and management

ISO/IEC 20000-1:2011, Clauses 4.5.2 and 4.5.3 include requirements for risk assessment, and for the treatment of risks associated with the SMS.

ISO/IEC 27001:2005, Clause 4.2.1, gives requirements for managing all aspects of risk associated with information security. The requirements are not limited to risks associated with the ISMS itself and include assessing and treating risks and other aspects of managing information security risk.

Even though risks are considered in both ISO/IEC 27001 and ISO/IEC 20000-1, the nature of these risks differs. ISO/IEC 20000-1 considers risks to the SMS and services, while ISO/IEC 27001 considers information security risk and how it affects the organization. The criteria for evaluation and treatment of risks can differ, depending on whether the risks are associated with delivery of a service, or specifically for information security. However, the method used to identify risks can be the same in both cases. Some risks considered by ISO/IEC 20000-1, e.g. the risk of a supplier not respecting the costs associated with an SLA, would not be considered as risks from the point of view of ISO/IEC 27001. Thus risks identified using ISO/IEC 20000-1 cannot be assumed to be relevant to information security, and vice versa.

The ownership of risk can also differ between the two approaches. For example, in ISO/IEC 20000-1 the service provider organization rarely owns all risks. A customer can be expected to approve residual risks as part of their SLA or the service continuity plan. In ISO/IEC 27001, the matter of risk ownership is not explicitly discussed, but in practice the organization is considered the owner of all information security risks.

Misunderstandings of risk management options arise because of the differences in the requirements for risk management between the two standards. When planning the integrated implementation of both standards, organizations should be mindful of any differences in risk criteria and the impact that these differences will have on risk treatment.

The organization should adopt one of the two approaches described below.

a) Use one common approach to risk management, including risk assessment, for both standards, avoiding duplication. For example, the risk of loss of availability of an information asset may be shared by the different parts of the integrated management system. This is the most efficient approach as it avoids duplication of effort.

b) Use separate risk assessment methodologies for the two standards. If this option is chosen, the organization should use terminology that differentiates risk assessment of the SMS and services from ISMS and information security risk assessment.

Where risk assessment and risk management are key to the organization, priority should be given to the implementation of ISO/IEC 27001, to take advantage of its risk assessment and risk management guidance. Whichever option is taken, the organization should use consistent and clear terminology. This may require expressing requirements from one or both of the standards differently from the published version(s). However, the organization should still ensure clear traceability to the requirements in both standards.

6.2.4 Differences in risk acceptance levels

Where a customer has entrusted their data or systems to the care of a third party, there can be differences between the customer's risk acceptance level and that of the third party. This is not explicitly covered in either standard, but the organization should be aware of the issues and to make a clear decision regarding levels of risk to be controlled by the different parties.

The key issues are described below.

a) The customer will have a view regarding the level of security which is acceptable for its information which is under the control of the third party. This might not match the level of security which the third party considers to be sufficient.

b) The third party will also have its own information, e.g. financial records. The third party will have a view regarding the level of security which is acceptable for this information.

c) The customer and the third party can be involved in different legal and regulatory enforcement environments, which vary by country or market sector. This can lead to different information security or risk perspectives.

The information security expectations and responsibilities of the organization's customers and third parties should be discussed at the earliest possible opportunity. These discussions are important both for the agreement of the scope of an implementation project, and equally when instituting operational controls for existing services. Any potential conflicts should be identified and decisions made and agreed, ideally before implementation.

6.2.5 Incident and problem management

The first point to discuss is that of terminology. In ISO/IEC 27001, there is a single term for unwanted events of interest: information security incident. In contrast, in ISO/IEC 20000-1 there are several specialized terms linked with incident management. For example, incident, information security incident, problem, known error, and major incident, see Annex B of this International Standard. These can all be information security incidents according to ISO/IEC 27001, depending on their characteristics.

ISO/IEC 27001 describes a single process to deal with all information security incidents.

ISO/IEC 20000-1 not only has a variety of terms, it also has a variety of mechanisms to manage these events, such as incident and service request management, major incident procedure and problem management. In ISO/IEC 20000-1 a single event can be managed by more than one of these processes and procedures during its lifecycle. ISO/IEC 20000-1 uses the ISO 9000:2005 definition for procedure as "a specified way to carry out an activity or process". For ISO/IEC 20000-1 process is a higher level than procedure, with procedures supporting a process.

Figure 3 illustrates the relationship between information security incident management in ISO/IEC 27001 and incident management in ISO/IEC 20000-1.

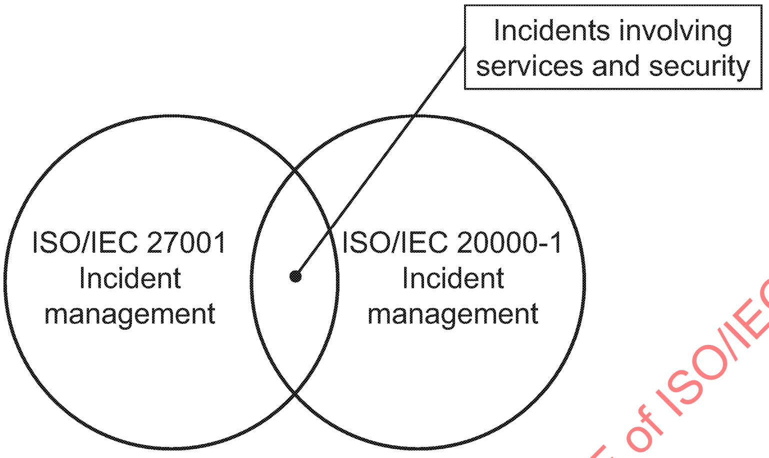
Incidents involving services and security
ISO/IEC 27001 Incident management
ISO/IEC 20000-1 Incident management

Figure 3 — Illustration of relationship between standards for incident management

There are events which ISO/IEC 27001 would classify as an information security incident, but which ISO/IEC 20000-1 would not classify as an incident. Two examples are given below.

a) A confidential document on marketing of a product is found on a desk after working hours, in violation of the information security policy. The document does not relate to service delivery in any way.

b) The lock for the door to a customer's office is found to be broken. This event could be considered an incident under ISO/IEC 27001. However this would not fall into the scope of ISO/IEC 20000-1 unless it provided access to information relevant to the requirements in ISO/IEC 20000-1:2011, Clause 6.6.

Equally, there are events which ISO/IEC 20000-1 would classify as an incident, but which are out of the scope of ISO/IEC 27001. For example:

a) scheduled maintenance exceeds SLA limits;

b) a user reports an incident due to slow service performance.

The primary overlap between the definitions of "incident" relates to what ISO/IEC 20000-1 refers to as "information security incidents", which can result in the loss of confidentiality, integrity and accessibility relating to a service.

In order to reconcile these views, the organization should decide how to handle the management of incidents which are in the scope of both management systems.

Problem management is defined in ISO/IEC 20000-1 as the process of identifying the root cause of one or more incidents to minimize or avoid the impact of incidents. In ISO/IEC 20000-1, this is a separate specific process. In ISO/IEC 27001 problem management is not explicitly covered, although it is alluded to in the requirements for information security incident management, risk treatment and corrective actions.

In an integrated management system, the problem management process should be defined. If an ISMS is implemented before the SMS, it can be useful to integrate the SMS best practices for problem management as part of the ISMS, due to its benefit to all management systems.

Both standards require the organization to analyse data and trends on incidents.

Incidents that involve an information security risk should be classified as information security incidents. It is equally important for conformity to both standards that the incident management process should reflect the need to conform to the additional requirements for information security in ISO/IEC 27001.

It should be noted that the control in ISO/IEC 27001:2005, A13.2.2 covers learning from security incidents, and is therefore a partial overlap with problem management in ISO/IEC 20000-1:2011, Clause 8.2. Moreover, the identification and evaluation of vulnerabilities required for an ISO/IEC 27001 information security risk assessment should be regarded as a data analysis process which can be used as an input to problem management.

The second issue to describe is the matter of response to an incident. Any organization should have the objective of quickly restoring service after an information security incident has affected a service. However, this can reduce the likelihood that a security incident is investigated in order to understand the cause. Care should be taken, when integrating an SMS and an ISMS, to ensure that the requirements for managing information security incidents are conformed to. For example, information security controls can include the collection, retention and provision of evidence for disciplinary or legal purposes. Further, both standards require compliance with legal and regulatory requirements.

It should be recognized that, in the case of an information security incident, the requirement to collect evidence can mean that the affected service cannot be restored within agreed service targets. ISO/IEC 20000-1 requires the service provider to take into account the urgency and impact of the incident. This can mean that additional time is required before an information security incident is resolved. The priority allocated to resolution should take into account the importance of collecting information security evidence that can otherwise be lost by the restoration of the service.

In some cases an information security incident will be a major incident, based on the definition of major incident agreed with the customer under ISO/IEC 20000-1:2011, Clause 8.1. According to the service reporting requirements in ISO/IEC 20000-1:2011, Clause 6.2 and the major incident management requirements in ISO/IEC 20000-1:2011, Clause 8.1, top management are informed of all major incidents. This includes those that are also information security incidents. This also ensures a properly trained, responsible individual is appointed to manage an information security incident. Within the integrated management system this event should then be managed as a major incident.

A major incident should not be routinely declared to allow a delay in resolution for the collection of evidence in the case of an information security incident. For example, if a website handling customer payments is found to have been compromised. Evidence collection and service restoration times should be adequately covered in service requirements, the catalogue of services and in service level agreements (SLAs).

The ISO/IEC 20000-1 definition of information security uses the word “accessibility” and the ISO/IEC 27001 definition uses the word “availability”. This difference is because the word “availability” is defined differently in the two standards, as described in Annex B.

6.2.6 Change management

ISO/IEC 27001:2005, A.10.1.2 and A.12.5.1 describe change management. Both A.10.1.2 and A.12.5.1 allow the organization to develop procedures to meet its specific needs.

ISO/IEC 20000-1:2011, Clause 9.2, Change management, includes requirements relating to risk. The requirements are supplemented by Clause 6.6.3, Information security changes and incidents. Clause 6.6.3 includes requirements for impact assessment of requested changes, to consider their effect upon existing information security controls.

To ensure that change management requirements are fulfilled, checklists for impact assessment or post-implementation review should be developed as part of the integrated management system based upon ISO/IEC 20000-1. This should ensure that all types of information security risk are reviewed as part of the change management process.

6.3 Potential gains

6.3.1 Use of the Plan-Do-Check-Act cycle

Both ISO/IEC 27001 and ISO/IEC 20000-1 refer explicitly to the Plan-Do-Check-Act (PDCA) cycle. This can be convenient, as the organization can follow the same principles whichever standard is to be implemented first.

PDCA is the basis for continual improvement in both standards, so continual improvement should be the focus of activities when implementing either or both of the two standards. It should be noted that the PDCA cycles can operate on different timescales, but if at all possible the organization should use a single integrated cycle to provide the same review or internal audit period.

6.3.2 Service level management and reporting

Service reporting covers a much wider base of activities than required for service level management. However, service reporting can support information security management by having service targets for information security incidents which are measured, trended and used in service reporting.

ISO/IEC 20000-1:2011, Clause 6.2 bullet b), states that the service reporting process should include relevant information about significant events, such as major incidents and nonconformities. Outputs from the ISO/IEC 20000-1 service reporting process can be a major advantage to maintaining and improving information security.

When implementing ISO/IEC 27001, details of information security controls are defined, and the effectiveness of these controls should be measured, see ISO/IEC 27001:2005, Clause 4.2.3 Monitor and review the ISMS. This also provides an opportunity for integration with the service reporting process of ISO/IEC 20000-1:2011, Clause 6.2, so that relevant and timely information can be used to maintain or improve information security. Customers can have a better understanding of the true performance of services and the SMS, including service management processes, if relevant information security control compliance levels and incident statistics are incorporated into reports.

Both ISO/IEC 27001 and ISO/IEC 20000-1 reports, whether for internal use or for customers, should be designed with these considerations in mind.

6.3.3 Management commitment

ISO/IEC 27001 describes information security in relation to stakeholders. The stakeholders referred to are parties with a vested interest in the organization where the ISMS is implemented. These parties can include staff, shareholders, customers, and possibly even regulatory authorities or the general public. ISO/IEC 20000-1 refers to customers and interested parties. Interested parties are a person or group having a specific interest in the performance or success of the service provider's activity or activities. Interested parties are therefore similar to "stakeholders", used in ISO/IEC 27001:2005.

Top management commitment is required to make the SMS effective. This includes ensuring that relationships with customer and other interested parties are successful. As such, the management commitment stated in ISO/IEC 27001 will support the customer focused approach in ISO/IEC 20000-1.

ISO/IEC 20000-1:2011 includes specific requirements for management commitment and management responsibilities, e.g. the requirements in Clauses 4.1.1 and 4.1.4. In contrast, ISO/IEC 27001:2005 is less specific about which roles should be responsible and accountable for the ISMS, e.g. the requirements Clauses 5.1 and 5.2.2. An integrated management system should take advantage of the specific nature of ISO/IEC 20000-1 and use its requirements to ensure that wider information security responsibilities are taken as seriously as service management responsibilities.

ISO/IEC 20000-1 states that, when presenting the management of improvements, the organization should assign responsibility for managing the improvement process to a specific role. In contrast, ISO/IEC 27001:2005, Clauses 4.2.4 and 8.1 refer to the organization handling this task, while Clause 5.1 includes requirements that the organization establishes roles and responsibilities for information security. The ISO/IEC 20000-1 requirement for explicit assignment of responsibility for managing improvements should be used to ensure that the management of improvements to information security is also assigned to a specific role.

6.3.4 Capacity management

Capacity management in ISO/IEC 20000-1:2011, Clause 6.5, includes a wider range of capacity concepts than ISO/IEC 27001, so some ISO/IEC 20000-1 requirements can be used to support an ISO/IEC 27001 implementation. For example, capacity management as described in ISO/IEC 20000-1 applies to both technical capacity and human resource capacity. Additionally, ISO/IEC 27001:2005, Clause 5.2, Resource management, can relate to capacity management, as capacity is access to sufficient resources to deal with reasonably foreseeable circumstances.

In ISO/IEC 27001:2005, Clause 3.2, availability is defined to mean both accessible and usable. Capacity management in ISO/IEC 20000-1:2011, Clause 6.5, supports both these aspects of availability. For example, if there is insufficient capacity, a service or service component can be inaccessible, e.g. if it is not possible to save a file because there is too little storage capacity. Alternatively, a service or service component can be so slow it is unusable, e.g. response time because there is too little network capacity.

The organization should be aware of this difference when cross-referencing requirements between the two standards. The organization should take into account the need to cross-reference ISO/IEC 20001:2011, Clauses 4.3 and 6.5 and relevant clauses in ISO/IEC 27001:2005, see Annex A of this International Standard. For example, the requirement to include the potential impact of statutory, regulatory, contractual or organizational changes in the capacity plan, required by ISO/IEC 20000-1:2011, Clause 6.5, should be cross-referenced with ISO/IEC 27001:2005, Clause A.10.1.

6.3.5 Management of third party risk

In ISO/IEC 27001, a third party, such as a customer, supplier or independent internal group, is outside the scope of the ISMS and is seen as a potential source of risk. Annex B of this International Standard includes a comparison of these terms, ISO/IEC 27001 describes controls which could be used to manage the security of these third parties in A.6.2.1 and A.6.2.3.

In contrast, in ISO/IEC 20000-1, other parties are entities not under the direct control of the service provider, but which contribute to the service in the scope of the SMS. Other parties are suppliers, internal groups or customers (when acting as suppliers). Other parties can contribute to a major part of the service, see ISO/IEC 20000-1:2011 Clause 4.2, Governance of processes operated by other parties. ISO/IEC 20000-1:2011, Clause 6.6, describes requirements for information security management. This includes the management of risk associated with a supplier, which can directly affect the customer organization’s information security. ISO/IEC 20000-1:2011, Clause 8.1 also refers to the incident and service request process for management of information security incidents, and the assessment of all changes to review the impact on information security controls.

When designing an integrated management system, there are two main considerations which affect the business relationship and supplier management processes with regards to managing third party risks. The two considerations are described below.

a) Contractual information security obligations should be an input to the risk assessment process. This process should contribute to the fulfilment of ISO/IEC 20000-1 requirements for the service provider to respond to business needs.

b) Information security should be covered when dealing with other parties, including customers acting as suppliers. This should be considered when a new or changed service is designed and the service catalogue and SLAs are discussed.

Other concepts covered in ISO/IEC 20000-1:2011, Clause 7.1, such as performance reviews, service changes, customer satisfaction management and complaint handling, can be applied to an integrated management system to strengthen it as a whole.

In summary, an integrated management system should follow the ISO/IEC 27001 approach to manage relationships with suppliers, but also comply with the requirement in ISO/IEC 20000-1:2011, Clause 6.6.2, Information security controls regarding supplier risk. Where the organization's assets are within the scope of the ISMS but some or all of these assets are controlled by another party, the organization should agree suitable contracts, SLAs or other documented agreements. This approach should ensure that the third party or other party applies appropriate controls.

6.3.6 Continuity and availability management

ISO/IEC 20000-1:2011, Clause 6.3, Service continuity and availability management, explicitly covers one part of the areas of concern for information security. Continuity and availability activities within an existing management system should be reviewed to see if they can usefully be extended to cover integrity and confidentiality management, and therefore manage information security for any service. Here, the detail could be drawn from ISO/IEC 20000-1 and the general principles from ISO/IEC 27001:2005, Clause A.14.

6.3.7 Supplier management

ISO/IEC 27001:2005 covers supplier management in different clauses, e.g. A.6.2.1, A.6.2.3, A.10.2, A.8 for human resources including contractors. ISO/IEC 20000-1:2011, Clause 4.2 includes requirement for governance of processes operated by other parties and Clause 7.2 includes requirements for supplier management. Supplier management under both standards can be combined effectively.

Clause 6.3.5 of this International Standard includes further information on managing risks associated with suppliers. For example, ISO/IEC 20000-1 risk assessments can be extended, using ISO/IEC 27001 concepts, to consider whether the security of the organization will be compromised by the addition or removal of a supplier, or by a particular alteration to the service which a supplier contributes to.

This should be considered even if the organization decides to implement only one of the standards.

6.3.8 Configuration management

The asset inventory in ISO/IEC 27001 is a repository of anything which has value (monetary or otherwise) to an organization and is in the scope of the ISMS, e.g. information, databases or processes.

The concept of the configuration management database (CMDB) in ISO/IEC 20000-1 is similar to the asset inventory in ISO/IEC 27001; but the scopes, and therefore perspectives, differ. Implementation of scope is discussed in ISO/IEC 20000-1:2011, Clause 4.5.1.

The requirements in ISO/IEC 20000-1:2011, Clause 9.1 can be used in creating and managing an ISMS. From the ISO/IEC 27001 perspective, the organization should manage the security of the CMDB, as this should be treated as an information asset.

ISO/IEC 20000-1:2011, Clause 9.1 also requires the CMDB to be secure to protect the accuracy of the data held. This includes a requirement for the maintenance of services and service component integrity. However, ISO/IEC 20000-1 does not draw a distinction between different levels of integrity. ISO/IEC 27001 can add value here, as it requires that the risks to systems, services and service components be evaluated, and acceptable levels of risk defined. The primary issue is whether the level of risk might be altered by a change, and, if so, whether that alteration raises risk to an unacceptable level.

Requirements for configuration baselines and master copies in ISO/IEC 20000-1 are actually controls, from the ISO/IEC 27001 perspective. These requirements should be considered when integrating risk management approaches. Some of them will affect decisions on whether or not to implement certain controls.

6.3.9 Release and deployment management

Conforming to the requirements for release and deployment management in ISO/IEC 20000-1:2011, Clause 9.3 does not ensure conformity with the ISO/IEC 27001 requirements for a release. Security issues can be accidentally introduced during this phase if ISO/IEC 27001 requirements are not followed. Examples include:

a) changes can be made to the operation of live system(s) which introduce information security flaws if release and deployment management does not take into account the possibility of malicious action;

b) managing test and live environments is often done by different groups, therefore a release process should ensure that the correct production role receives data from the test group, to avoid risks to confidential data.

This is particularly important during emergency releases. In these situations, a different and possibly volatile release and deployment process is often used, due to time and/or resource constraints. The risks of compromising information security are therefore increased. Information security risks should always be properly managed by following approved information security processes, regardless of which release and deployment process is to be used.

Release and deployment management can be improved through the selection of the controls in ISO/IEC 27001:2005, A.10.1.4 Separation of development, test and operational facilities, and A.10.3.2, System acceptance.

6.3.10 Budgeting and accounting

The budgeting and accounting requirements in ISO/IEC 20000-1:2011, Clause 6.4, cannot be directly mapped to any ISO/IEC 27001 requirement. In ISO/IEC 27001, the requirement for provision of resources and the output of the management review (which requires a decision to be made on about resource needs) can benefit from consideration of financial resources and a defined budgeting process.

Annex A
(informative)

Correspondence between ISO/IEC 27001:2005 and ISO/IEC 20000-1:2011

A.1 General

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

Clauses where there is overlap in most of the requirements and details between ISO/IEC 27001 and ISO/IEC 20000-1 are highlighted in light grey.
Clauses where there is overlap in most of the requirements and details between ISO/IEC 27001 Annex A and ISO/IEC 20000-1 are highlighted in dark grey.
Areas with no shading are those where there is no significant overlap.

Table A.1 — Correspondence between ISO/IEC 27001 and ISO/IEC 20000-1:2011

ISO/IEC 27001	ISO/IEC 20000-1
Introduction	Introduction
General	No direct equivalent
Process approach	No direct equivalent
Compatibility with other management systems	No direct equivalent
1 Scope	1 Scope
1.1 General	1.1 General
1.2 Application	1.2 Application
2 Normative references	2 Normative references
3 Terms and definitions	3 Terms and definitions
4 Information security management system	4 Service management system general requirements
4.1 General requirements	No direct equivalent
4.2 Establishing and managing the ISMS	4.5 Establish and improve the SMS
No direct equivalent	4.5.1 Define scope
No direct equivalent	4.5.2 Plan the SMS (Plan)
4.2.2 Implement and operate the ISMS	4.5.3 Implement and operate the SMS (Do)
4.2.3 Monitor and review the ISMS	4.5.4 Monitor and review the SMS (Check)
4.2.4 Maintain and improve the ISMS	4.5.5 Maintain and improve the SMS (Act)
4.3 Documentation requirements	4.3 Documentation management
4.3.1 General	4.3.1 Establish and maintain documents
4.3.2 Control of documents	4.3.2 Control of documents
4.3.3 Control of records	4.3.3 Control of records
5 Management responsibility	4.1 Management responsibility
5.1 Management commitment	4.1.1 Management commitment
No direct equivalent	4.1.2 Service management policy
No direct equivalent	4.1.3 Authority, responsibility and communication
No direct equivalent	4.1.4 Management representative
No direct equivalent	4.2 Governance of processes operated by other parties

ISO/IEC 27001	**ISO/IEC 20000-1**
5.2 Resource management	4.4 Resource management
5.2.1 Provision of resources	4.4.1 Provision of resources
5.2.2 Training, awareness and competence	4.4.2 Human resources
6 Internal ISMS audit	4.5.4.2 Internal audit
7 Management review of the ISMS	4.5.4.3 Management review
7.1 General	4.5.4.3 Management review
7.2 Review input	4.5.4.3 Management review
7.3 Review output	4.5.4.3 Management review
8 ISMS improvement	4.5.5 Maintain and improve the SMS (Act)
8.1 Continual improvement	4.5.5.1 General
	4.5.5.2 Management of improvements
8.2 Corrective action	4.5.5.1 General
	4.5.5.2 Management of improvements
	8 Resolution processes
8.3 Preventative action	4.5.5.1 General
	4.5.5.2 Management of improvements
	8 Resolution processes
No direct equivalent	5 Design and transition of new or changed services
No direct equivalent	5.1 General
No direct equivalent	5.3 Design and development of new or changed services
No direct equivalent	5.4 Transition of new or changed services
No direct equivalent	6 Service delivery processes
A.10.2.1 Service delivery	6.1 Service level management
A.10.2.2 Monitoring and review of third party services	6.2 Service reporting
No direct equivalent	6.3 Service continuity and availability management
No direct equivalent	6.4 Budgeting and accounting for services
A.10.2.3 Managing changes to third party services	5.2 Plan new or changed services
A.10.3.1 Capacity management	6.5 Capacity management
ISO/IEC 27001	6.6 Information security management
No direct equivalent	7 Relationship processes
No direct equivalent	7.1 Business relationship management
No direct equivalent	7.2 Supplier management
A.13 Information security incident management	8.1 Incident and service request management
No direct equivalent	8.2 Problem management
No direct equivalent	9 Control processes
No direct equivalent (only partly in several controls)	9.1 Configuration management
A.12.5.1 Change control processes	9.2 Change management
No direct equivalent	9.3 Release and deployment management
Annex A Control objectives and controls	(partly covered above, see detailed breakdown)
Annex B OECD principles and this International Standard	No direct equivalent
Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard	No direct equivalent

Annex B
(informative)

Comparison of ISO/IEC 27000:2009 and ISO/IEC 20000-1:2011 terms

In Table B.1 the International Standards are referred to without the year of publication in the column of "Comments on usage of the terms in both standards", for the sake of brevity. Table B.1 provides a comparison of terms defined in ISO/IEC 27000:2009, which is the Glossary for ISO/IEC 27001:2005, terms used in ISO/IEC 27001, and terms defined or used in ISO/IEC 20000-1:2011. Areas where the terms are defined differently between ISO/IEC 27000 and ISO/IEC 20000-1 are highlighted in light grey.

Table B.1 — Comparison of terms

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Access control	2.1 means to ensure that access to assets (2.3) is authorized and restricted based on business and security requirements	Not defined	No direct equivalent
Accountability	2.2 responsibility of an entity for its actions and decisions	Not defined	The word accountability is used in ISO/IEC 20000-1 in its normal English sense: responsibility, being required to explain or defend one's actions or conduct, the acknowledgment and assumption of responsibility The word accountability is important to the requirements in ISO/IEC 20000-1, Clause 4.2, i.e. "…by….a) demonstrating accountability for the processes and authority to require adherence to the processes;"

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Asset	2.3 anything that has value to the organization NOTE There are many types of assets, including: a) information (2.18); b) software, such as a computer program; c) physical, such as computer; d) services; e) people, and their qualifications, skills, and experience; and f) intangibles, such as reputation and image.	Not defined	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, person, etc. There is little use of the word asset in ISO/IEC 20000-1: Clause 4.1.4: “[Management representative] has the authorities and responsibilities that include: d) ensuring that assets, including licences, used to deliver services are managed according to statutory and regulatory requirements and contractual obligations; Clause 6.4: “There shall be policies and documented procedures for: a) budgeting and accounting for service components including at least: 1) assets - including licences - used to provide the services;” Clause 6.6.2: “The service provider shall implement and operate physical, administrative and technical security controls in order to: a) preserve confidentiality, integrity and accessibility of information assets;” Clause 9.1: “There shall be a defined interface between the configuration management process and financial asset management process. NOTE The scope of the configuration management process excludes financial asset management.”
Attack	2.4 attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset (2.3)	Not defined	No direct equivalent
Authentication	2.5 provision of assurance that a claimed characteristic of an entity is correct	Not defined	No direct relevance to this information security related term, "*authentication*'; which is used in ISO/IEC 27001 in the technical sense. '*Authentication*" is not similar to "verification" in the management system life cycle activities
Authenticity	2.6 property that an entity is what it claims to be	3.11 NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.	Referenced in ISO/IEC 20000-1 but not used thereafter.

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Availability	2.7 property of being accessible and usable upon demand by an authorized entity	3.1 ability of a service or service component to perform its required function at an agreed instant or over an agreed period of time NOTE Availability is normally expressed as a ratio or percentage of the time that the service or service component is actually available for use by the customer to the agreed time that the service should be available. 3.11 NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. NOTE 2 The term "availability" has not been used in this definition because it is a defined term in this part of ISO/IEC 20000 which would not be appropriate for this definition. NOTE 3 Adapted from ISO/IEC 27000:2009.	See "information security". Availability is often considered to be central to service management and plays a prominent role in ISO/IEC 20000-1 in the aspect of assessing the quality of services provided. See ISO/IEC 20000-1, Clause 6.3. The difference between the two definitions is not large, but because of the importance placed on "availability" in service management, the difference is noteworthy. A direct consequence of the difference between the two meanings of availability is that the ISO/IEC 27000 definition of information security was adapted for ISO/IEC 20000-1 by the use of accessibility instead of availability.
Business continuity	2.8 processes (2.31) and/or procedures (2.30) for ensuring continued business operations	Not defined	Service continuity is used in ISO/IEC 20000-1 as a subset of business continuity. See service continuity
Confidentiality	2.9 property that information is not made available or disclosed to unauthorized individuals, entities, or processes (2.31)	Not defined	No direct equivalent

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Configuration baseline	Not defined	3.2 configuration information formally designated at a specific time during a service or service component's life NOTE 1 Configuration baselines, plus approved changes from those baselines, constitute the current configuration information. NOTE 2 Adapted from ISO/IEC/IEEE 24765:2010.	The term is used once in ISO/IEC 20000-1, Clause 9.1, as in: "….A configuration baseline of the affected CIs shall be taken before deployment of a release into the live environment.
Configuration item (CI)	Not defined	3.3 element that needs to be controlled in order to deliver a service or services	CIs are prominent in ISO/IEC 20000-1 and are considered to be a component of the service. CIs can be one or part of a service component. An information asset can be a CI. See ISO/IEC 20000-1, definition 3.27 service component.
Configuration management database (CMDB)	Not defined	3.4 data store used to record attributes of CIs, and the relationships between CIs, throughout their lifecycle	Depending on the approach being adopted by the organization, a CMDB can be used to hold the inventory of assets. See ISO/IEC 27001, Annex A, Clause A.7.1.1.
Continual improvement	Not defined	3.5 recurring activity to increase the ability to fulfil service requirements NOTE Adapted from ISO 9000:2005.	ISO/IEC 20000-1, Clause 4.1.2, requires a policy on continual improvement, as part of the service management policy. The PDCA cycle, as included in the Introduction of ISO/IEC 27001, is very similar to ISO 9001 and to ISO/IEC 20000-1. (cf. ISO/IEC 27001, Clause 4.2.4 and ISO/IEC 20000-1, Clause 4.5.5, for example).

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Control	2.10 means of managing risk (2.34), including policies (2.28), procedures (2.30), guidelines (2.16), practices or organizational structures, which can be administrative, technical, management, or legal in nature ISO 31000:2009 2.26 control measure that is modifying risk (2.1) NOTE 1 Controls include any process, policy, device, practice, or other actions which modify risk. NOTE 2 Controls may not always exert the intended or assumed modifying effect. [ISO Guide 73:2009, definition 3.8.1.1]	Not defined	The word control is used in ISO/IEC 20000-1 as both a noun and verb, but not defined as a special term, so the normal English meaning applies: noun: authority or charge; power to influence or guide, take control, a means of limitation. (controls) a device for operating, regulating, or testing (a machine, system, etc). Verb: (controlled, controlling) to have or exercise power over someone or something, to regulate, to limit, to operate, regulate or test (a machine, system, etc). All but two uses of "control" as a noun are in ISO/IEC 20000-1, Clause 6.6, Information security management, the other uses are in Clauses 4.3.2 and 4.4.3, which is text taken almost unchanged from ISO 9001:2008). Control is used as a verb in many places, usually as: "control of XXX process" or "X shall be controlled by Y".
Control objective	2.11 statement describing what is to be achieved as a result of implementing controls (2.10)	Not defined	The noun "objective" is used in ISO/IEC 20000-1 in the normal English sense: a thing aimed at or wished for; a goal. There is at most a tenuous link between the use of "control objective" in ISO/IEC 27001 and the use in ISO/IEC 20000-1, Clauses 4 of phrases such as "service management objectives" or Clause 6.6, “information security management objectives”.
Corrective action	2.12 action to eliminate the cause of a detected nonconformity or other undesirable situation [ISO 9000:2005]	3.6 action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity or other undesirable situation NOTE Adapted from ISO 9000:2005.	The same term is used in both standards, but there are differences in meaning. It is not always possible or desirable to eliminate the cause, instead it can be better or more cost effective to avoid recurrence. See preventive action in ISO/IEC 20000-1, definition 3.18.
Customer	Not defined	3.7 organization or part of an organization that receives a service or services NOTE 1 A customer can be internal or external to the service provider's organization. NOTE 2 Adapted from ISO 9000:2005.	In ISO/IEC 20000-1, the customer can additionally act as supplier.

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Document	Not defined	3.8 information and its supporting medium [ISO 9000:2005] EXAMPLES Policies, plans, process descriptions, procedures, service level agreements, contracts or records. NOTE 1 The documentation can be in any form or type of medium. NOTE 2 In ISO/IEC 20000, documents, except for records, state the intent to be achieved.	No direct equivalent
Effectiveness	2.13 extent to which planned activities are realized and planned results achieved [ISO 9000:2005]	3.9 extent to which planned activities are realized and planned results achieved [ISO 9000:2005]	Identical.
Efficiency	2.14 relationship between the results achieved and how well the resources have been used	Not defined	This word is used in its normal English sense, and only once, in the introduction of ISO/IEC 20000-1. There are no requirements concerning efficiency.
Event	2.15 occurrence of a particular set of circumstances [ISO/IEC Guide 73:2002]	Not defined	This word event is used in ISO/IEC 20000-1, in its normal English sense: something that occurs or happens. For examples, see ISO/IEC 20000-1, Clause 6.2: ” significant events” or 6.3.2 Service continuity and availability plans: “in the event of a major loss of service”. This usage is similar to ISO/IEC 27001, so broadly comparable. See Information security event.

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Guideline	2.16 recommendation of what is expected to be done to achieve an objective	Not defined	See other parts of ISO/IEC 20000. While ISO/IEC 20000-1 contains normative requirements, all other parts of ISO/IEC 20000 are informative International Standards or Technical Reports.
Impact	2.17 adverse change to the level of business objectives achieved	Not defined	Use of the word "impact" in both standards is broadly similar. 'Impact" is used 26 times in ISO/IEC 20000-1, in the normal English language sense of: Impact, noun: a strong effect or impression This use of "impact" is less specific in ISO/IEC 20000-1 than how "impact" is used in ISO/IEC 27001. Most uses in ISO/IEC 20000-1, are associated with a risk or an actual negative circumstance, e.g. the definition 3.15 Known error and in Clause 5: “The service provider shall use this process for all new services and changes to services with the potential to have a major impact on services or the customer. “ or Clause 6.3.2: “The service provider shall assess the impact of requests for change on the service continuity plan(s) and the availability plan(s). “

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Incident	See Information security incident	3.10 unplanned interruption to a service, a reduction in the quality of a service or an event that has not yet impacted the service to the customer	There is a significant difference between the use of "incident" in ISO/IEC 27001 series and in ISO/IEC 20000-1. The word "incident" is used in ISO/IEC 27001 to mean "something that has gone wrong with the security of the in-scope environment". In ISO/IEC 20000-1 the word "incident" has a defined meaning and is more specific than in ISO/IEC 27001. In ISO/IEC 20000-1 "incident" is one of a series of related terms and is not only associated with information security incidents. Other related terms are: 3.19 Problem root cause of one or more incidents The root cause is not usually known at the time a problem record is created and the problem management process is responsible for further investigation. 3.15 Known error problem that has an identified root cause or a method of reducing or eliminating its impact on a service by working around it Major incident (not a defined term) either an incident (or problem) that is considered to be of the highest category of impact. Each of "incident", "problem", and "major incident" are managed differently and are subject to different requirements. 'Known error" is a problem where the underlying cause is understood and is managed by the problem management process, which includes requirements that apply once a problem has become a known error. 'Major incident" is managed by the incident and service request management process, with a requirement that there is a special procedure for managing "major incidents". See Information security incident

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Information asset	2.18 knowledge or data that has value to the organization	Not defined	This term is not a defined term but is used in ISO/IEC 20000-1, e.g. Clause 6.6.2: "The service provider shall implement and operate physical, administrative and technical information security controls in order to: a) preserve confidentiality, integrity and accessibility of information assets;" See "asset".
Information security	2.19 preservation of confidentiality (2.13), integrity (2.36) and availability (2.10) of information NOTE In addition, other properties, such as authenticity (2.9), accountability (2.2), non-repudiation (2.49), and reliability (2.56) can also be involved.	3.11 preservation of confidentiality, integrity and accessibility of information NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. NOTE 2 The term "availability" has not been used in this definition because it is a defined term in this part of ISO/IEC 20000 which would not be appropriate for this definition. NOTE 3 Adapted from ISO/IEC 27000:2009.	In ISO/IEC 20000-1, the word availability cannot be used in the definition of information security in 3.11, because availability is a defined term with a different meaning (see "availability'). The definition for information security has therefore been adapted to use the term accessibility instead. Accessibility was taken from the ISO/IEC 27000 definition of availability "property of being accessible and usable upon demand by an authorised entity".
Information security event	2.20 identified occurrence of a system, service or network state indicating a possible breach of information security (2.19) policy (2.28) or failure of controls (2.10), or a previously unknown situation that may be security relevant	Not defined	Information security event is only used in ISO/IEC 20000-1, as part of the definition 3.12: information security incident. Additionally, 2.15 event (not information security event) is also used in: a) the definition of risk – see 3.25, which includes NOTES 3 and 4 referring that refer to events. b) the definition of service continuity (3.28) c) ISO/IEC 20000-1, Clause 6.2 Service reporting d) ISO/IEC 20000-1, Clause 6.3.2 Service continuity and availability plans See event: one or more events can form part of a security incident.

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Information security incident	2.21 single or series of unwanted or unexpected information security events (2.20) that have a significant probability of compromising business operations and threatening information security (2.19)	3.12 single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security [ISO/IEC 27000:2009]	The ISO/IEC 20000-1 definition 3.12 includes the ISO/IEC 27000 term information security incident. ISO/IEC 20000-1, Clause 6.6.3, includes a requirement: Information security incidents shall be managed using the incident management procedures, with a priority appropriate to the information security risks. This does not cater for "things that have gone wrong with the service" where the cause is a problem, i.e. root cause of one or more incidents, when the root cause is not usually known at the time a problem record is created and the problem management process is responsible for further investigation. These are managed by the problem management process, not the incident management and service request process. Major [information security] incidents are managed by the incident and service request process referred to. The variation in the way the term is used in both standards is more complex than a security event or incident being a sub-set or special type of [service management] incident. See Clause 6.2.5 of this International Standard.
Information security incident management	2.22 processes (2.31) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (2.21)	Not defined	See: 'Incident' 'Information security incident' 'Known error' 'Problem'
Information security management system (ISMS)	2.23 part of the overall management system (2.26), based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security (2.19)	Not defined	See "service management system" and "management system".
Information security risk	2.24 potential that a threat (2.45) will exploit a vulnerability (2.46) of an asset (2.3) or group of assets and thereby cause harm to the organization	Not defined	See "risk". Information security risk is not defined but is used in the information security management section of ISO/IEC 20000-1, Clause 6.6.1.

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Integrity	2.25 property of protecting the accuracy and completeness of assets (2.3)	Not defined.	This word integrity is used in ISO/IEC 20000-1 in its normal English sense: the quality or state of being whole and unimpaired. (e.g. see ISO/IEC 20000-1, Clause 6.6.2: “The service provider shall implement and operate physical, administrative and technical information security controls in order to: a) preserve confidentiality, integrity and accessibility of information assets.” ISO/IEC 20000-1, Clause 9.1 includes the requirements: “There shall be a documented procedure for recording, controlling and tracking versions of CIs. The degree of control shall maintain the integrity of services and service components taking into consideration the service requirements and the risk associated with the CIs". “Changes to CIs shall be traceable and auditable to ensure integrity of the CIs and the data in the CMDB.” ISO/IEC 20000-1, Clause 9.3 includes the requirements: “The release shall be deployed into the live environment so that the integrity of hardware, software and other service components is maintained during deployment of the release”
Interested party	Not defined	3.13 person or group having a specific interest in the performance or success of the service provider's activity or activities EXAMPLES Customers, owners, management, people in the service provider's organization, suppliers, bankers, unions or partners. NOTE 1 A group can comprise an organization, a part thereof, or more than one organization. NOTE 2 Adapted from ISO 9000:2005.	See "service provider".

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Internal group	Not defined	3.14 part of the service provider's organization that enters into a documented agreement with the service provider to contribute to the design, transition, delivery and improvement of a service or services NOTE The internal group is outside the scope of the service provider's SMS.	See "service provider".
Known error	Not defined	3.15 problem that has an identified root cause or a method of reducing or eliminating its impact on a service by working around it	See "incident" and "problem".
Management system	2.26 framework of policies (2.28), procedures (2.30), guidelines (2.16) and associated resources to achieve the objectives of the organization	Management system is defined in Note 1 of the definition of service management system: NOTE 1 A management system is a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives.	Used in ISO/IEC 20000-1 to refer to "other management systems", ISO/IEC 20000-1 is referred to as a "service management system".
Non-repudiation	2.27 ability to prove the occurrence of a claimed event (2.15) or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event (2.15) or action and involvement of entities in the event (2.15)	Not defined or used	No direct equivalent

Term	ISO/IEC 27000:2009	ISO/IEC 20000-1:2011	Comments on usage of the term in both standards
Organization	Not defined	3.17 group of people and facilities with an arrangement of responsibilities, authorities and relationships EXAMPLES Company, corporation, firm, enterprise, institution, charity, sole trader, association, or parts or combination thereof. NOTE 1 The arrangement is generally orderly. NOTE 2 An organization can be public or private. [ISO 9000:2005]	ISO/IEC 20000-1 uses the term "service provider" and "organization" for different entities, so the difference is significant in any explanations for integrated management system. See "service provider'
Policy	2.28 overall intention and direction as formally expressed by management	Not defined	The word policy is used in ISO/IEC 20000-1 in its normal English sense: (policies) a plan of action, usually based on certain principles, decided on by a body or individual, a principle or set of principles on which to base decisions, a course of conduct to be followed. Policies are used in ISO/IEC 20000-1 for management direction. Several are required by ISO/IEC 20000-1, including a service management policy. Usage is largely the same across both standards.
Preventive action	2.29 action to eliminate the cause of a potential nonconformity or other undesirable potential situation [ISO 9000:2005]	3.18 action to avoid or eliminate the causes or reduce the likelihood of occurrence of a potential nonconformity or other potential undesirable situation NOTE Adapted from ISO 9000:2005.	The definitions differ, in that the ISO/IEC 20000-1 definition has been extended to include: preventative action which does not eliminate the cause, but works round it in some way to avoid there being an impact; and preventative action which does not eliminate the cause, but works round it in some way to avoid there being an impact. The same term is used in both standards, but there are differences in meaning. It is not always possible or desirable to take preventive action in service management. Instead, it can be better / more cost effective to avoid recurrence. Therefore, for ISO/IEC 20000-1, the ISO 9000 definition was adapted to allow for this possibility. This links to corrective action in ISO/IEC 20000-1, definition 3.6 and ISO/IEC 27000 definition 2.12.