INTERNATIONAL STANDARD

ISO/IEC 27013

Second edition
2015-12-01

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

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

Reference number
ISO/IEC 27013:2015(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 Scope

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

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

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

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

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

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

2 Normative references

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

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

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

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

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

3 Terms, definitions and abbreviated terms

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

The following abbreviations apply.

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

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

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

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

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

— terms used in ISO/IEC 27001;

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

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

4.1 Understanding the International Standards

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

4.2 ISO/IEC 27001 concepts

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

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

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

4.3 ISO/IEC 20000-1 concepts

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

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

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

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

4.4 Similarities and differences

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

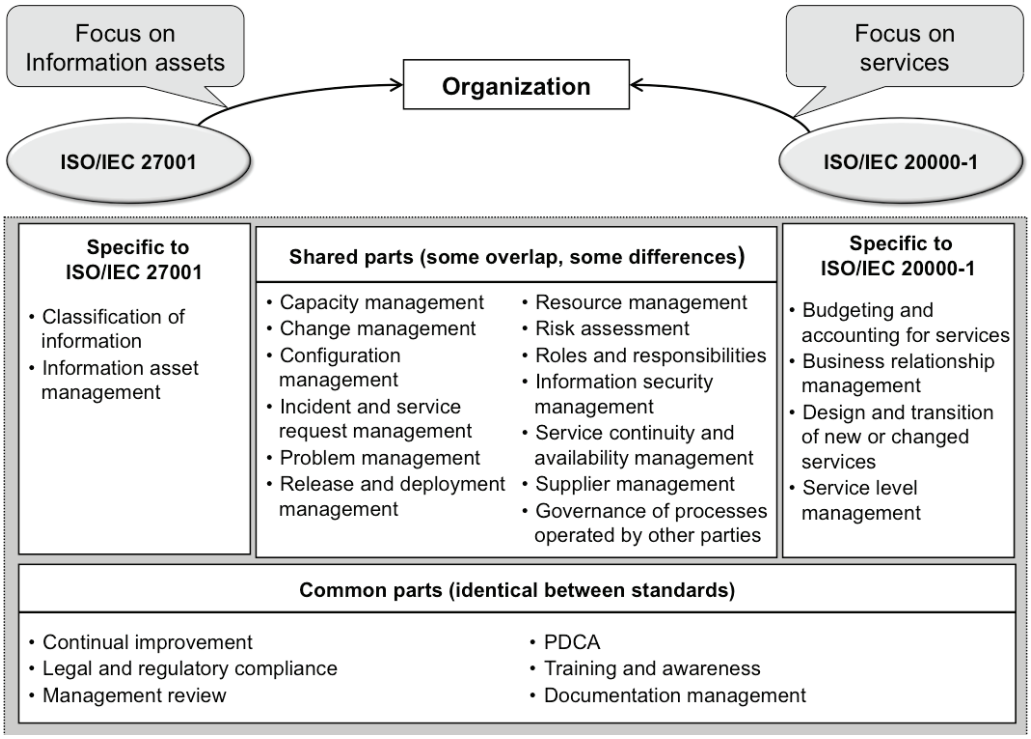

Figure 1 — Comparison between concepts in ISO/IEC 27001 and ISO/IEC 20000-1

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

5 Approaches for integrated implementation

5.1 General

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

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

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

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

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

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

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

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

d) elements that are to remain separate;

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

f) the impact on technology in use;

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

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

i) education and training in the integrated management system;

j) phases and sequence of implementation activities.

5.2 Considerations of scope

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

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

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

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

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

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

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

5.3 Pre-implementation scenarios

5.3.1 General

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

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

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

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

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

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

These considerations are illustrated in the following scenarios.

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

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

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

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

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

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

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

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

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

a) scope;

b) organizational structure;

c) policies;

d) planning activities;

e) authorities and responsibilities;

f) practices;

g) risk management methodologies;

h) relevant processes;

i) procedures;

j) terms and definitions;

k) resources.

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

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

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

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

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

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

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

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

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

   1) start with a very broad outline view;

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

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

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

6 Integrated implementation considerations

6.1 General

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

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

6.2 Potential challenges

6.2.1 The usage and meaning of asset

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

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

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

CIs. For example, a data cable can be a CI. Although it is not information, the cable is the resource used for carrying information and thus is relevant to risk assessment in ISO/IEC 27001. For an integrated management system, information can be used by, or be part of, a service in ISO/IEC 20000-1.

Neither of the standards requires every CI or instance of information to be listed individually. They can be grouped into types, such as hardware, or documents. As part of this activity, 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 categorised and identified. This is to ensure that unambiguous references can be made to assets. If the term asset is used to refer to information, 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).

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 changes in external and internal issues are required to be considered during the management review of the ISMS (ISO/IEC 27001:2013, 9.3), and several aspects of service design, transition and delivery are covered in ISO/IEC 27001:2013, 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, 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 27001:2013, 6.1 and Clause 8 specify requirements for assessing and treating 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. ISO/IEC 27001:2013, 6.1 provides detail on how to carry out information security risk assessment and treatment.

Even though risks are considered in both ISO/IEC 27001 and ISO/IEC 20000-1, the nature of these risks can differ. 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 specific to delivery of a service, or to 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 a service level agreement (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 treatment 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 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.

c) Use a common approach for assessing and treating those risks that affect both information security and service management, and separate risk assessment and treatment methodologies for risks that are specific to information security and service management.

Whatever approach is taken, subdividing risk assessment and treatment to separately consider risks that affect both information security and service management, and risks that affect either information security or service management can improve management system efficiency.

Where risk assessment and risk treatment are critical to the organization, priority should be given to the implementation of ISO/IEC 27001 to take advantage of its risk assessment and risk treatment requirements. 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 specified 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 should 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 that is acceptable for its information that is under the control of the third party. This might not match the level of security that the third party considers to be sufficient.

b) The third party itself will also have its own information, e.g. financial records. The third party will have a view regarding the level of security 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 during the agreement of the scope of an implementation project and 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 of comparison is that of terminology. In ISO/IEC 27001, the term for unwanted events of interest is information security incident. In contrast, in ISO/IEC 20000-1, there are several specialised terms linked with incident management. For example, incident, information security incident, problem, known error and major incident (see Annex B). These can all be information security incidents, according to ISO/IEC 27001, depending on their characteristics.

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

ISO/IEC 20000-1 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 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 2 illustrates the relationship between information security incident management in ISO/IEC 27001 and incident management in ISO/IEC 20000-1.

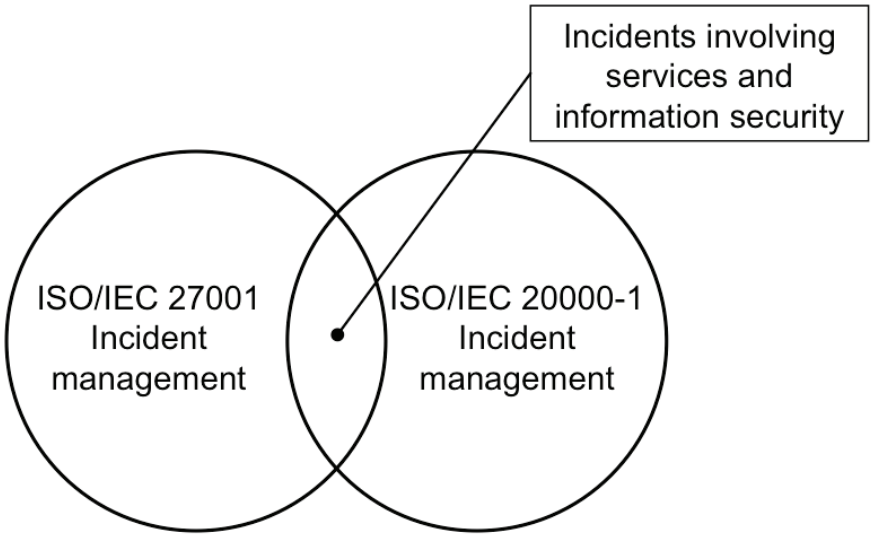

Figure 2 — Illustration of relationship between standards for incident management

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 services or service delivery in any way.

b) The lock for the door to a customer’s office is found to be broken. This event can be considered an incident under ISO/IEC 27001. However, this would not fall into the scope of ISO/IEC 20000-1 unless the event impacted information relevant to the requirements in ISO/IEC 20000-1:2011, 6.6 or the services supported by the SMS.

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. Examples are as follows:

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 those incidents that are in the scope of both management systems.

Problem management is defined in ISO/IEC 20000-1 as the process for identifying the root cause of one or more incidents to minimise 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 and risk treatment.

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 benefits for 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 management in ISO/IEC 27001.

It should be noted that the control in ISO/IEC 27001:2013, A.16.1.6 covers learning from security incidents and is therefore a partial overlap with problem management in ISO/IEC 20000-1:2011, 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 procedure, which can be used as an input to problem management.

The second point of comparison 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 applicable legal and regulatory requirements.

It should be recognised 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 specifies a requirement for the service provider to take into account the urgency and impact of the incident. This can mean that additional time is required to collect evidence 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 can be a major incident, based on the definition of major incident agreed with the customer specified in ISO/IEC 20000-1:2011, 8.1. According to the service reporting requirements in ISO/IEC 20000-1:2011, 6.2 and the major incident management requirements in ISO/IEC 20000-1:2011, 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. Some information security incidents should not be handled using the standard major incident process, but by the information security management function; for example, an internal breach of security which requires police investigation and forensic examination. These types of incidents require their existence to be limited to a smaller group than would normally be the case.

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 International Standards, as described in Annex B.

6.2.6 Change management

ISO/IEC 27001:2013, 7.5.3 requires changes to documented information relating to the ISMS to be controlled. ISO/IEC 27001:2013, 8.1 also required the organization to control planned changes.

ISO/IEC 27001:2013, A.12.1.2, A.14.2.2, 14.2.3, 14.2.4, and A.15.2.2 describe change management. These Clauses allow the organization to develop procedures to meet its specific needs.

ISO/IEC 20000-1:2011, 9.2 includes requirements relating to risk. The requirements are supplemented by 6.6.3. 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 the requirements specified in 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

ISO/IEC 20000-1 refers explicitly to the Plan-Do-Check-Act (PDCA) cycle. Though ISO/IEC 27001 does not mention this cycle explicitly, its main clauses are structured around the PDCA cycle. This can assist the organization, as it can use the detail in ISO/IEC 20000-1 to support the implementation of the integrated management system. The elements of the PDCA cycle can be mapped to the structure of ISO/IEC 27001 as appropriate.

6.3.2 Service level management and reporting

Service reporting covers a much wider base of activities than is specified 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, 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 27001:2013, 9.1). This also provides an opportunity for integration with the service reporting process of ISO/IEC 20000-1:2011, 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.

Reports to support the ISMS and SMS, 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 “interested parties”. These 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”, as used in ISO/IEC 20000-1, is therefore similar to “interested parties” as used in ISO/IEC 27001.

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

ISO/IEC 20000-1 specifies that, when presenting the management of improvements, the organization should assign responsibility for managing improvements to the SMS and services to a specific role. In

contrast, ISO/IEC 27001:2013, 5.1 requires top management to promote continual improvement, while 5.2 requires top management to commit to continual improvement. ISO/IEC 27001:2013, 6.1.1 and 7.1 refer to the organization managing various aspects of continual improvement, with 10.2 stating that the organization shall carry out continual improvement of its ISMS.

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 assigned to a specific role.

6.3.4 Capacity management

Capacity management in ISO/IEC 20000-1:2011, 6.5 includes a wider range of capacity concepts than ISO/IEC 27001, so some requirements specified in ISO/IEC 20000-1 can be used to support an ISO/IEC 27001 implementation. For example, capacity management as specified in ISO/IEC 20000-1 applies to both technical capacity and human resource capacity.

In ISO/IEC 27000:2014, 2.10, availability is defined to mean both accessible and usable. Capacity management in ISO/IEC 20000-1:2011, 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 20000-1:2011, 4.3 and 6.5 and relevant clauses in ISO/IEC 27001. See Annex A. For example, the requirement to include the potential impact of statutory, regulatory, contractual or organizational changes in the capacity plan, specified in ISO/IEC 20000-1:2011, 6.5, should be cross-referenced with ISO/IEC 27001:2013, A.12.1.3.

6.3.5 Management of third party risk

In ISO/IEC 27001, a third party, such as a customer or supplier, is inside the scope of the ISMS as it is a potential source of risk. Annex B includes a comparison of these terms. ISO/IEC 27001 describes controls that could be used to manage the security of suppliers in A.15

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 can be 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, 4.2. ISO/IEC 20000-1:2011, 6.6 specifies 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, 8.1 also refers to the incident and service request management 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 management 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 defined and agreed.

Other concepts covered in ISO/IEC 20000-1:2011, 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 should also conform to the requirements specified in ISO/IEC 20000-1:2011, 6.6.2. 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 other party applies appropriate controls.

6.3.6 Continuity and availability management

ISO/IEC 20000-1:2011, 6.3 explicitly covers one part of the areas of concern for information security. Continuity and availability management 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 27001:2013, A.17.2.

ISO/IEC 27001:2013, A.17 considers exclusively how to manage information security when invoking the business continuity process. This concept can very usefully be used to augment the service continuity requirements specified in ISO/IEC 20000-1.

6.3.7 Supplier management

ISO/IEC 27001:2013 covers supplier management in A.15. It also references employees and contractors across a large number of clauses, e.g. A.7.2, A.15.2 and A.16.1.3. ISO/IEC 20000-1:2011, 4.2 includes requirements for governance of processes operated by other parties and 7.2 includes requirements for supplier management. Supplier management under both International Standards can be combined effectively.

6.3.5 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 to which a supplier contributes.

This should be considered even if the organization decides to address the requirements of only one of the International Standards.

6.3.8 Configuration management

The asset inventory in ISO/IEC 27001:2013, A.8.1.1 is a repository of anything that 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, 4.5.1.

The requirements in ISO/IEC 20000-1:2011, 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 asset.

ISO/IEC 20000-1 does not draw a distinction between different levels of integrity. ISO/IEC 27001:2013 can add value here, as 6.1 requires that the risks to systems, services and service components be evaluated, and levels of risk determined. 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. ISO/IEC 27001:2013, 6.2 requires that information security objectives be defined and achieved. These objectives should include a definition of the acceptable level of risk to availability, integrity and confidentiality of the information within the scope of the ISMS.

Requirements for configuration baselines and master copies specified 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 specified in ISO/IEC 20000-1:2011, 9.3 does not ensure conformity with ISO/IEC 27001:2013 requirements for security in development and support processes, A.14.2. Security issues can be accidentally introduced during this phase if ISO/IEC 27001 requirements are not followed. Examples include the following:

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, so a release and deployment management 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 management procedure can be used, due to time and/or resource constraints. The risks of compromising information security can therefore be increased. Information security risks should always be properly managed by following approved information security processes, regardless of which release and deployment management procedure is to be used.

Release and deployment management can be improved through the selection of the controls in ISO/IEC 27001:2013, A.12.1.4 and A.14.2.9.

6.3.10 Budgeting and accounting

The budgeting and accounting for services requirements specified in ISO/IEC 20000-1:2011, 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 about resource needs) can benefit from consideration of financial resources and a defined budgeting and accounting process.

Annex A
(informative)

Correspondence between ISO/IEC 27001 and ISO/IEC 20000-1

A.1 General

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

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 27001:2013, 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

Based on SC27 comparison ISO/IEC 27001	Based on SC40 comparison ISO/IEC 20000 -1
not requirements so not included (yet)	Introduction
not requirements so not included (yet)	1 Scope
not requirements so not included (yet)	1.1 General
not requirements so not included (yet)	1.2 Application
2 Normative references	2 Normative references
3 Terms and definitions	3 Terms and definitions
4. Context of the organization	Many – see below
4.1 Understanding the organization and its context	4.1.1 Management commitment
4.2 Understanding the needs and expectations of interested parties	5.2 Para. 1, Plan new or changed services, 5.4 Para. 1, Transition of new or changed services, 6.2, Para. 1, Service reporting, 6.3.1, Para. 1, Service continuity and availability requirements, 6.5, Para.1 Capacity management, 7.1, Paras. 1 and 3, Business relationship management, 8.1 Para. 5, Incident and service request management, 9.2 Paras. 8, 10, Penultimate para, Change management, 9.3 Paras. 2, 5, Release and deployment management
4.3 Determining the scope of the information security management system	1.2 Applicability, 4.2 Governance of processes operated by other parties, 4.3 Documentation management, 4.5.1 Define scope, 4.5.2 Plan the SMS (Plan) (please also see ISO/IEC 20000-3)
4.4 Information security management system	No direct equivalent
5 Leadership	4.1 Management responsibility
5.1 Leadership and commitment	4.1.1 Management commitment
5.1 a) Leadership and commitment	4.1.1 a) Management commitment
5.1 b) Leadership and commitment	4.1.1 b) Management commitment, 4.2 Governance of processes operated by other parties, 7.2 Business relationship management
5.1 c) Leadership and commitment	4.1.1 e) Management commitment, 4.4.1 Para. 1, Provision of resources 4.5.2 g) Plan the SMS (Plan), 4.5.4.3 c) Management review, 5.2 d) Plan new or changed services, 5.3 c) Design and development of new or changed services, 6.4 a) 1), 2) Budgeting and accounting for services, 6.5 Para. 2 Capacity management,
5.1 d) Leadership and commitment	4.1.1 Management commitment 4.1.2 Service management policy
5.1 e) Leadership and commitment	4.1.1 b) Management commitment
5.1 f) Leadership and commitment	4.1.1 Management commitment 4.1.3 Authority, responsibility and communication
5.1 g) Leadership and commitment	4.1.2 c) Service management policy
5.1 h) Leadership and commitment	4.1.3 Authority, responsibility and communication
5.2 Policy	4.1.1 a), b) Management commitment, 4.1.2 Service management policy,

Table A.1 — *(continued)*

Based on SC27 comparison ISO/IEC 27001	Based on SC40 comparison ISO/IEC 20000 -1
	4.3.1 Establish and maintain documents 4.3.2 Control of documents, 4.3.3 Control of records
5.3 Organizational roles, responsibilities and authorities	4.1.3 Authority, responsibility and communication, 4.1.4 Management representative 4.3.3 Control of records 4.5.4.2 Internal audit
6 Planning	4.5.2 Plan the SMS (Plan)
6.1 Actions to address risks and opportunities	See below
6.1.1 Actions to address risks and opportunities – General	Risk references: 4.5.2 j) Plan the SMS (Plan), 4.5.3 d) Implement and operate the SMS (Do), 4.5.4.3 e) Management review, 4.5.5.2 a) Management of improvements, 5.3 Design and development of new or changed services, 5.2 f) Plan new or changed services, 6.3.1 Para. 1 Service continuity and availability requirements, 6.6.1 c) Information security policy, 6.6.3 a) Information security changes and incidents, 8.2 Problem management 9.2 Para. 8 Change management.
6.1.2 Information security risk assessment	The equivalent to this is ISO/IEC 20000-1, Clause 6.6, but there are many references to risk with similar requirements: 4.5.2 j) Plan the SMS (Plan), 4.5.3 d) Implement and operate the SMS (Do), 4.5.4.3 e) Management review, 5.2 f) Plan new or changed services, 6.3.1 Para. 1 Service continuity and availability requirements, 6.6.1 c), d) Information security policy, 6.6.3 a), Para. 2 Information security changes and incidents, 9.2 Para. 8 Change management.
6.1.3 Information security risk treatment	There is no direct equivalent to this in ISO/IEC 20000-1, except for Clause 6.6, but there are many references to risk with similar requirements: 4.1.1 g) Management commitment, 4.3.1 Establish and maintain documents 4.5.2 j) Plan the SMS (Plan), 4.5.3 d) Implement and operate the SMS (Do), 5.2 f) Plan new or changed services, 6.6.2 d), Para. 2 Information security controls
6.2 Information security objectives and plans to achieve them	4.1.1 Management commitment
7.1 Resources	4.1.1 e) Management commitment, 4.4 Resource management
7.2 Competence	4.4.2 Human resources 4.3 Documentation management
7.3 Awareness	4.1 Management responsibility, 4.4.2 d) Human resources
7.4 Communication	4.1.1 a), c), d) Management responsibility 4.1.3 b) Authority, responsibility and communication 4.3.2 b), Control of documents, 4.5.4.1 last para. General, 4.5.4.2, last para, Internal audit, 5.2 c) Plan new or changed services, 5.4 last para. Transition of new or changed services 6.2 last para. Service reporting, 6.6.1, a) Information security policy, 7.1, para. 3, Business relationship management, 7.2, j), Supplier management, 9.2 Para. 10, Change management,
7.5 Documented information	4.3 Documentation management
7.5.1 General	4.3.1 Establish and maintain documents
7.5.2 Creating and updating	4.3.2 Control of documents 4.3.3 Control of records
7.5.3 Control of documented information	4.3.2 Control of documents 4.3.3 Control of records
8 Operation	4.5 Establish and improve the SMS Clauses 5 to 9
8.1 Operational planning and control	4.2 Governance of processes operated by other parties, 4.5 Establish and improve the SMS, Also many points on Clauses 6 to 9
8.2 Information security risk assessment	There is no direct equivalent to this in ISO/IEC 20000-1, except for Clause 6.6, but there are many references to risk with similar requirements:

Table A.1 — *(continued)*

Based on SC27 comparison ISO/IEC 27001	Based on SC40 comparison ISO/IEC 20000 -1
	4.5.2 j) Plan the SMS (Plan), 4.5.3 d) Implement and operate the SMS (Do), 4.5.4.3 e) Management review, 5.2 f) Plan new or changed services, 6.3.1 Para. 1 Service continuity and availability requirements, 6.6.1 c), d) Information security policy, 6.6.3 a), Para. 2 Information security changes and incidents, 9.2 Para. 8 Change management.
8.3 Information security risk treatment	There is no direct equivalent to this in ISO/IEC 20000-1, except for Clause 6.6, but there are many references to risk with similar requirements: 4.1.1 g) Management commitment, 4.3.1 Establish and maintain documents 4.5.2 j) Plan the SMS (Plan), 4.5.3 d) Implement and operate the SMS (Do), 5.2 f) Plan new or changed services, 6.6.2 d), Para. 2 Information security controls,
9 Performance evaluation	See below
9.1 Monitoring, measurement, analysis and evaluation	4.1.2 a), d), f) Service management policy, 4.3.3 para. 1 Control of records, 4.5.3 f) Implement and operate the SMS (Do), 4.5.4.1 General, 6.2 Service reporting, 8.2 Problem management
9.2 Internal audit	4.5.4.2 Internal audit 4.3.1 Establish and maintain documents 4.3.3 Control of records
9.3 Management review	4.1.2 c) Service management policy, 4.3.3 Control of records 4.5.4.3 Management review
10 Improvement	4.5.5 Maintain and improve the SMS (Act)
10.1 Nonconformity and corrective action	4.1.2 c) Service management policy 4.3.1 Establish and maintain documents g), 4.3.3 Control of records 4.5.4 Monitor and review the SMS (Check), 4.5.5 Maintain and improve the SMS (Act), 8.2 Problem management
10.2 Continual improvement	4.1.2 c) Service management policy, 4.5.5 Maintain and improve the SMS (Act), 9.2 Last para. Change management
A.5 Information security policies	See below
A.5.1 Management direction for information security	6.6.1 Information security policy
A.6 Organization of information security	See below
A.6.1 Internal organization	Not specified in 20000-1
A.6.2 Mobile devices and teleworking	Not specified in 20000-1
A.7 Human resource security	See below
A.7.1 Prior to employment	Not specified in 20000-1
A.7.2 During employment	6.6.1 Information security policy
A.7.3 Termination and change of employment	Not specified in 20000-1
A.8 Asset management	See below
A.8.1 Responsibility for assets	6.6.2 Information security controls
A.8.2 Information classification	Not specified in 20000-1
A.8.3 Media handling	Not specified in 20000-1
A.9 Access control	See below
A.9.1 Business requirements of access control	Not specified in 20000-1
A.9.2 User access management	Not specified in 20000-1
A.9.3 User responsibilities	Not specified in 20000-1
A.9.4 System and application access control	Not specified in 20000-1
A.10 Cryptography	See below
A.10.1 Cryptographic controls	Not specified in 20000-1
A.11 Physical and environmental security	See below
A.11.1 Secure areas	Not specified in 20000-1
A.11.2 Equipment	Not specified in 20000-1
A.12 Operations security	See below
A.12.1 Operational procedures and responsibilities	Not specified in 20000-1
A.12.2 Protection from malware	Not specified in 20000-1
A.12.3 Backup	6.3 Service continuity and availability management
A.12.4 Logging and monitoring	Not specified in 20000-1
A.12.5 Control of operational software	Not specified in 20000-1
A.12.6 Technical vulnerability management	Not specified in 20000-1
A.12.7 Information systems audit considerations	Not specified in 20000-1
A.13 Communications security	See below
A.13.1 Network security management	Not specified in 20000-1
A.13.2 Information transfer	Not specified in 20000-1
A.14 System acquisition, development and maintenance	See below

Table A.1 — *(continued)*

Based on SC27 comparison ISO/IEC 27001	Based on SC40 comparison ISO/IEC 20000 -1
A.14.1 Security requirements of information systems	6.6.3 Information security changes and incidents
A.14.2 Security in development and support processes	6.6.3 Information security changes and incidents
A.14.3 Test data	Not specified in 20000-1
A.15 Supplier relationships	See below
A.15.1 Information security in supplier relationships	6.6.2 Information security controls
A.15.2 Supplier service delivery management	4.2 Governance of processes operated by other parties 7.2 Supplier management
A.16 Information security incident management	See below
A.16.1 Management of information security incidents and improvements	6.6.3 Information security changes and incidents 8.1 Incident and service request management
A.17 Information security aspects of business continuity management	See below
A.17.1 Information security continuity	Not specified in 20000-1
A.17.2 Redundancies	6.3 Service continuity and availability management
A.18 Compliance	See below
A.18.1 Compliance with legal and contractual requirements	6.6.1 Information security policy
A.18.2 Information security reviews	6.6.1 Information security policy 6.6.2 Information security controls 6.6.3 Information security changes and incidents

Annex B
(informative)

Comparison of ISO/IEC 27000 and ISO/IEC 20000-1 terms

B.1 General

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, which is the Glossary for ISO/IEC 27001, terms used in ISO/IEC 27001, and terms defined or used in ISO/IEC 20000-1. 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	ISO/IEC 20000-1	Comments on usage of the term in both standards
Access control	2.1 means to ensure that access to assets is authorised and restricted based on business and security requirements	Not defined	No direct equivalent
Attack	2.3 attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset	Not defined	No direct equivalent
Audit	2.5 systematic, independent and documented process (2.61) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled Note 1 to entry: An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines). Note 2 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.	Not defined	Broadly the same meaning in both standards
Authentication	2.7 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	2.8 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.

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Availability	2.9 property of being accessible and usable upon demand by an authorised 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.	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.
Confidentiality	2.12 property that information is not made available or disclosed to unauthorised individuals, entities, or processes (2.61)	Not defined	No direct equivalent
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.

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
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).
Control	2.16 measure that is modifying risk (2.68) NOTE 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk NOTE 2 to entry: 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 taken almost verbatim 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	2.17 statement describing what is to be achieved as a result of implementing controls (2.16)	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”.
Correction	2.18 action to eliminate a detected nonconformity (2.53)	Not defined	No direct equivalent
Corrective action	2.19 action to eliminate the cause of a nonconformity (2.53) and to prevent recurrence [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.	Both based upon ISO 9000:2005 See “preventive action”

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
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. In ISO/IEC 27001, a customer is an interested party.
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	2.24 extent to which planned activities are realised and planned results achieved	3.9 extent to which planned activities are realised and planned results achieved [ISO 9000:2005]	Identical.
Event	2.25 occurrence or change of a particular set of circumstances [ISO/IEC Guide 73:2009] NOTE 1: An event can be one or more occurrences, and can have several causes. NOTE 2: An event can consist of something not happening. NOTE 3: An event can sometimes be referred to as an "incident" or "accident".	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 that in ISO/IEC 27001, so is broadly comparable. See "information security event"

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	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 refer to "information security incident" (see definition in this annex). 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"

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Information security	2.33 preservation of confidentiality (2.12), integrity (2.40) and availability (2.9) of information NOTE 1: In addition, other properties, such as authenticity (2.8), accountability), non-repudiation (2.54), and reliability (2.62) 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.	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 continuity	2.34 processes (2.61) and procedures (2.33) for ensuring continued information security operations	Not defined	ISO/IEC 27000 focuses upon the concept of maintaining information security operations during a business continuity event, as distinct from maintaining all services. Service continuity is used in ISO/IEC 20000-1 as a subset of business continuity. See "service continuity"
Information security event	2.35 identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, 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.

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Information security incident	2.36 single or a series of unwanted or unexpected information security events (2.36) that have a significant probability of compromising business operations and threatening information security (2.33)	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]	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	2.37 processes (2.61) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (2.36)	Not defined	See: “incident” “information security incident” “known error” “problem"
Integrity	2.40 property of accuracy and completeness	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”

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Interested party	2.41 person or organization (2.57) that can affect,or be affected by, or perceive themselves to be affected by a decision or activity	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". ISO/IEC 27000 places emphasis upon the effect to/by an interested party, whereas ISO/IEC 20000-1 emphasises their interest as the key criterion.
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	2.46 set of interrelated or interacting elements to establish policies (2.60) and objectives (2.56) and processes (2.61) to achieve those objectives. NOTE 1: A management system can address a single discipline or several disciplines. NOTE 2: The system elements include the organization's structure, roles and responsibilities, planning, operation, etc. NOTE 3: The scope of a management system may include the whole of an organization, specific and identified sections of the organization, or one or more functions across a group of organizations.	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.	Broadly the same meaning in both standards

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Non-repudiation	2.54 ability to prove the occurrence of a claimed event or action and its originating entities	Not defined or used	No direct equivalent
Organization	2.57 Person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives (2.56) Note 1 to entry: The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.	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 an integrated management system. In ISO/IEC 27001, the organization may be part of a larger entity, such as a company or charity. See "service provider".
Policy	2.60 intentions and direction of an organization (2.57) as formally expressed by its top management (2.84)	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	Not defined	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 ISO/IEC 20000-1 definition has been extended from the dictionary definition of the two terms (as used by default in the 2700x series) to include preventative action which does not eliminate the cause, but works round it in some way to avoid there being an impact. 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 2.19.
Problem	Not defined	3.19 root cause of one or more incidents NOTE 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.	See "incident" and "known error".

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Procedure	Not defined	3.20 specified way to carry out an activity or a process [ISO 9000:2005] NOTE Procedures can be documented or not.	The definition used by ISO/IEC 20000-1 is based on that in ISO 9000. They are broadly similar. Only the NOTE differs, i.e. procedures could be undocumented, but ISO/IEC 20000-1 references to procedures are all to "documented procedure". Those procedures that are part of a plan are documented as part of the plan.
Process	2.61 set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2005]	3.21 set of interrelated or interacting activities which transforms inputs into outputs [ISO 9000:2005]	Both based on ISO 9000:2005, the same.
Record	Not defined or used in the main text of ISO/IEC 27001	3.22 document stating results achieved or providing evidence of activities performed [ISO 9000:2005] EXAMPLES Audit reports, incident reports, training records or minutes of meetings.	The ISO/IEC 20000-1 definition is based on ISO 9000:2005. ISO/IEC 27001 uses the phrase “documented information” instead of the term “record”.
Release	Not defined or used	3.23 collection of one or more new or changed CIs deployed into the live environment as a result of one or more changes	No direct equivalent
Request for change	Not defined or used	3.24 proposal for a change to be made to a service, service component or the service management system NOTE A change to a service includes the provision of a new service or the removal of a service which is no longer required.	ISO/IEC 27001, Annex A refers to "change management" as a control in A.10.1.2 Many controls in ISO/IEC 27001 refer to the management or control of changes. For example: A.8.3, A.10.1, A.10.2.3, A.12.5.1
Reliability	2.62 property of consistent intended behaviour and results	Referred to in 3.11 information security: NOTE 1 In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.	This word “reliability” is used in ISO/IEC 20000-1 in its normal English sense: trustworthiness. See ISO/IEC 20000-1, Clause 9.1: “The CMDB shall be managed to ensure its reliability and accuracy, including control of update access.”

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Risk	2.68 effect of uncertainty on objectives [SOURCE: ISO Guide 73:2009] Note 1 to entry: An effect is a deviation from the expected – positive or negative. Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of, an event (2.25) its consequence (2.14) or likelihood (2.45). Note 3 to entry: Risk is often characterized by reference to potential events (2.25) and consequences (2.14), or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences (2.14) of an event (including changes in circumstances) and the associated likelihood (2.45) of occurrence. Note 5 to entry: In the context of information security management systems, information security risks can be expressed as effect of uncertainty on information security objectives. Note 6 to entry: Information security risk is associated with the potential that threats (2.83) will exploit vulnerabilities (2.89) of an information asset or group of information assets and thereby cause harm to an organization.	3.25 effect of uncertainty on objectives NOTE 1 An effect is a deviation from the expected — positive and/or negative. NOTE 2 Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). NOTE 3 Risk is often characterized by reference to potential events (2.17) and consequences (2.18), or a combination of these. NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (2.19) of occurrence. NOTE 5 Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood. [ISO Guide 73:2009, definition 1.1]	There is limited explicit use of "risk" in ISO/IEC 20000, although many proactive aspects of service management are aimed at reducing risks. ISO/IEC 27000 adds in specific interpretations of an information security risk, introducing the concept of vulnerabilities and threats. It also states that information security risks can be described in terms of how they affect information security objectives, rather than general organizational objectives. It should be noted that the concept of "risk" adopted in ISO/IEC 27001 under revision is the same as in ISO/IEC 20000-1, based on ISO 31000. See "vulnerability"

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Risk acceptance	2.69 informed decision to take a particular risk (2.68) [SOURCE: ISO Guide 73:2009] Note 1 to entry: Risk acceptance can occur without risk treatment (2.79) or during the process of risk treatment. Note 2 to entry: Accepted risks are subject to monitoring (2.52) and review (2.65).	Not defined	The phrase "acceptance of risk" is not defined or used in ISO/IEC 20000-1. However, in ISO/IEC 20000-1 there are requirements to define the criteria for accepting risk in the service management plan, Clause 4.5.2 and in the information security management process, Clause 6.6.1. Similar concepts are in Clause 5.4, in requirements for use of acceptance criteria.
Risk analysis	2.70 process to comprehend the nature of risk (2.68) and to determine the level of risk (2.44) [ISO Guide 73:2009] NOTE 1 Risk analysis provides the basis for risk evaluation (2.74) and decisions about risk treatment (2.79). NOTE 2 Risk analysis includes risk estimation.	Not defined	See "risk assessment". Special care should be applied; risk analysis is definitely not the same as "risk acceptance". See ISO/IEC 27005 for further information
Risk assessment	2.71 overall process (2.61) of risk identification (2.75), risk analysis (2.70) and risk evaluation (2.74) [ISO Guide 73:2009]	Not defined	References in ISO/IEC 20000-1 are to the risk assessment related to services. For example: Clause 4.5.3: (Implement and operate the SMS (Do)) includes "...d) identification, assessment and management of risks to the services;" Clause 5.2 (Plan new or changed services) includes f) identification, assessment and management of risks; Clause 6.6.1: "d) ensure that information security risk assessments are conducted at planned intervals;"

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Risk communication	2.72 risk communication and consultation continual and iterative processes that an organization conducts to provide, share or obtain information, and to engage in dialogue with stakeholders (2.82) regarding the management of risk (2.68) NOTE 1 The information can relate to the existence, nature, form, likelihood, significance, evaluation, acceptability and treatment of risk. NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: . a process which impacts on a decision through influence rather than power; and . an input to decision making, not joint decision making.	Not defined	Not used in ISO/IEC 20000-1 in any way relating to risk.
Risk criteria	2.73 terms of reference against which the significance of risk (2.68) is evaluated [ISO Guide 73:2009] NOTE 1 Risk criteria are based on organizational objectives, and external and internal context. NOTE 2 Risk criteria can be derived from standards, laws, policies and other requirements.	Not defined	Used in ISO/IEC 20000-1 in a similar way to its use in ISO/IEC 27001, e.g. ISO/IEC 20000-1, Clause 4.5.2" "The service management plan shall contain or include a reference to…) approach to be taken for the management of risks and the criteria for accepting risks;". The concept is similar for both standards, but has greater significance for ISO/IEC 27001 than for ISO/IEC 20000.

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Risk evaluation	2.74 process (2.61) of comparing the results of risk analysis (2.70) with risk criteria (2.73) to determine whether the risk (2.68) and/or its magnitude is acceptable or tolerable [ISO Guide 73:2009] NOTE Risk evaluation assists in the decision about risk treatment (2.79).	Not defined	See "risk assessment"
Risk identification	2.75 process of finding, recognizing and describing risks (2.68) [SOURCE: ISO Guide 73:2009] Note 1 to entry: Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Note 2 to entry: Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholders' needs.	Not defined	See "risk assessment"
Risk management	2.76 coordinated activities to direct and control an organization (2.57) with regard to risk (2.68)	Not defined	Broadly the same meaning in both standards
Risk owner	2.78 person or entity with the accountability and authority to manage a risk (2.68) [SOURCE: ISO Guide 73:2009]	Not defined	Broadly the same meaning in both standards

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Risk treatment	2.79 process (2.61) to modify risk (2.68) [ISO/IEC Guide 73:2009] Note 1 to entry: Risk treatment can involve: — avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; — taking or increasing risk in order to pursue an opportunity; — removing the risk source; — changing the likelihood; — changing the consequences; — sharing the risk with another party or parties (including contracts and risk financing); and — retaining the risk by informed choice. Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". Note 3 to entry: Risk treatment can create new risks or modify existing risks.	Not defined	The term "risk treatment" is not used in ISO/IEC 20000-1; this term is covered by the term "risk management" (see examples in "risk assessment").
Service	Not defined	3.26 means of delivering value for the customer by facilitating results the customer wants to achieve NOTE 1 Service is generally intangible. NOTE 2 A service can also be delivered to the service provider by a supplier, an internal group or a customer acting as a supplier.	No direct equivalent

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Service component	Not defined	3.27 single unit of a service that when combined with other units will deliver a complete service EXAMPLES Hardware, software, tools, applications, documentation, information, processes or supporting services. NOTE A service component can consist of one or more CIs.	No direct equivalent
Service continuity	Not defined	3.28 capability to manage risks and events that could have serious impact on a service or services in order to continually deliver services at agreed levels	See "vulnerability", "risks" and "business continuity". Service continuity is normally seen as a subset of business continuity.
Service level agreement (SLA)	Not defined	3.29 documented agreement between the service provider and customer that identifies services and service targets NOTE 1 A service level agreement can also be established between the service provider and a supplier, an internal group or a customer acting as a supplier. NOTE 2 A service level agreement can be included in a contract or another type of documented agreement.	This term is not used in ISO/IEC 27001. However, the concept is adopted in relation to the control objective A.10.2 when security aspects of the service delivered and maintained by a third party are considered, e.g. control A.10.2.1(agreed service continuity levels)
Service management	Not defined	3.30 set of capabilities and processes to direct and control the service provider's activities and resources for the design, transition, delivery and improvement of services to fulfil the service requirements	Control objective A.10.2 of ISO/IEC 27001 is related to this term

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Service management system SMS	Not defined	3.31 management system to direct and control the service management activities of the service provider NOTE 1 A management system is a set of interrelated or interacting elements to establish policy and objectives and to achieve those objectives. NOTE 2 The SMS includes all service management policies, objectives, plans, processes, documentation and resources required for the design, transition, delivery and improvement of services and to fulfil the requirements in this part of ISO/IEC 20000. NOTE 3 Adapted from the definition of "quality management system" in ISO 9000:2005.	The term "information security management system (ISMS)" is used in ISO/IEC 27001 to describe the organization in scope for information security management. See "organization".
Service provider	Not defined	3.32 organization or part of an organization that manages and delivers a service or services to the customer NOTE A customer can be internal or external to the service provider's organization.	"Service provider" in ISO/IEC 20000-1, definition 3.32, is the organization that is aiming to fulfil the requirements in ISO/IEC 20000-1. This term is used because it draws a distinction between the service provider and other groups, which are customers, other parties (suppliers, internal groups, customers, when acting as suppliers) external organizations, interested parties or providers of products or tools that support operation of the SMS. A service provider can be part of a larger organization or the whole of an organization.
Service request	Not defined	3.33 request for information, advice, access to a service or a pre-approved change	No direct equivalent
Service requirement	Not defined	3.34 needs of the customer and the users of the service, including service level requirements and the needs of the service provider	Service requirement is defined in ISO/IEC 20000-1, definition 3.34. In ISO/IEC 27001 "requirement" is used with its normal English meaning of: a need, something that is asked for, essential, ordered. It is not used in ISO/IEC 27001 as "service requirements", although there are several uses of "security requirements", legal or regulatory requirement, etc.

Table B.1 (*Continued*)

Term	ISO/IEC 27000	ISO/IEC 20000-1	Comments on usage of the term in both standards
Supplier	Not defined	3.35 organization or part of an organization that is external to the service provider's organization and enters into a contract with the service provider to contribute to the design, transition, delivery and improvement of a service or services or processes NOTE Suppliers include designated lead suppliers but not their sub-contracted suppliers.	ISO/IEC 20000-1 includes references to and requirements for the management of: a) suppliers b) lead suppliers (who manage sub-contracted suppliers) c) internal groups (contributing to the service) d) customers (when acting as suppliers). All contribute to the overall service and are managed by the service provider: Supplier management covers suppliers / lead suppliers (and via lead suppliers, sub-contracted suppliers) Service level management covers management of internal groups and customers, when acting as suppliers. ISO/IEC 27001 uses the term “supplier” only once.
Threat	2.83 potential cause of an unwanted incident, which may result in harm to a system or organization	Not defined	In ISO/IEC 20000-1, the term "threatening" is used once, in definition 3.12: “information security incident: single or a series of, unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security”
Top management	2.84 person or group of people who directs and controls an organization (2.57) at the highest level Note 1 to entry: Top management has the power to delegate authority and provide resources within the organization. Note 2 to entry: If the scope of the management system (2.46) covers only part of an organization (2.57) then top management refers to those who direct and control that part of the organization (2.57).	3.36 person or group of people who direct and control the service provider at the highest level NOTE Adapted from ISO 9000:2005.	In ISO/IEC 27000, “top management” can refer to a person, or group of people, who is/are not at the highest level of the whole organization, but are instead at the top of that part of the organization which is in scope for the ISMS. The organization can also have a role other than service provider. See “organization”
Transition	Not defined	3.37 activities involved in moving a new or changed service to or from the live environment	A link exists between transition, as used in ISO/IEC 20000-1, Clause 5 and the way in which some changes are controlled according to ISO/IEC 27001. Control processes, described in ISO/IEC 20000-1, Clauses 5 and 9, are also closely linked to this concept. ISO/IEC 27001 handles change management in the following clauses: A.10.1.2 Change management of operational procedures and responsibilities A.10.2.3 Managing changes to third party services
Vulnerability	2.89 weakness of an asset or control (2.16) that can be exploited by one or more threats (2.83)	Not defined or used	No direct equivalent

Bibliography

[1] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[2] ISO/IEC/TS 15504-8, *Information technology — Process assessment — Part 8: An exemplar process assessment model for IT service management*

[3] ISO 19011, *Guidelines for auditing management systems*

[4] ISO/IEC 20000-2, *Information technology — Service management — Part 2: Guidance on the application of service management systems*

[5] ISO/IEC 20000-3, *Information technology — Service management — Part 3: Guidance on scope definition and applicability of ISO/IEC 20000-1*

[6] ISO/IEC/TR 20000-4, *Information technology — Service management — Part 4: Process reference model*

[7] ISO/IEC/TR 20000-5, *Information technology — Service management — Part 5: Exemplar implementation plan for ISO/IEC 20000-1*

[8] ISO/IEC/TR 20000-9, *Information technology — Service management — Part 9: Guidance on the application of ISO/IEC 20000-1 to cloud services*

[9] ISO/IEC/TR 90006, *Information technology — Guidelines for the application of ISO 9001:2008 to IT service management and its integration with ISO/IEC 20000-1:2011*

[10] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*

[11] ISO/IEC 27003, *Information technology — Security techniques — Information security management system implementation guidance*

[12] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Measurement*

[13] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*

[14] ISO/IEC 27006, *Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems*

[15] ISO/IEC 27007, *Information technology — Security techniques — Guidelines for information security management systems auditing*

[16] ISO/IEC/TR 27008, *Information technology — Security techniques — Guidelines for auditors on information security controls*

[17] ISO/IEC 27010, *Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications*

[18] ISO/IEC 27014, *Information technology — Security techniques — Governance of information security*

[19] ISO 31000, *Risk management — Principles and guidelines*

[20] ISO Guide 73:2009, *Risk management — Vocabulary*

ICS 03.080.99; 35.020; 35.040

Price based on 39 pages