INTERNATIONAL STANDARD

ISO/IEC 27013

Third edition
2021-11

Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

Sécurité de l'information, cybersécurité et protection de la vie privée — Recommandations pour la mise en œuvre intégrée de l'ISO/IEC 27001 et de l'ISO/IEC 20000-1

Reference number
ISO/IEC 27013:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This third edition cancels and replaces the second edition (ISO/IEC 27013:2015), which has been technically revised. The main change compared with the previous edition is the alignment with ISO/IEC 20000-1:2018.

A list of all parts in the ISO/IEC 27000 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The relationship between information security management and service management is so close that many organizations already recognize 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 International Standard and then make further improvements to achieve conformity with the requirements of another.

There are a number of advantages for an organization in ensuring its management system takes into account both the service lifecycle and the protection of the organization's information. These benefits can be experienced whether one International Standard is implemented before the other, or ISO/IEC 27001 and ISO/IEC 20000-1 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) credibility to internal and external customers, and other interested parties of the organization, of effective and secure services;

b) lower cost of implementing, maintaining and auditing an integrated management system, where effective and efficient management of both services and information security are part of an organization's strategy;

c) reduction in implementation time due to the integrated development of processes supporting both service management and information security management;

d) better communication, increased reliability and improved operational efficiency through elimination of unnecessary duplication;

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

f) an organization certified for ISO/IEC 27001 can more easily fulfil the requirements for information security specified in ISO/IEC 20000-1:2018, 8.7.3, as ISO/IEC 27001 and ISO/IEC 20000-1 are complementary in requirements.

This document is based on ISO/IEC 27001:2013 and ISO/IEC 20000-1:2018.

This document is intended for use by persons who intend to integrate ISO/IEC 27001 and ISO/IEC 20000-1, and who are familiar with both, either or neither of those International Standards.

This document does not reproduce content of ISO/IEC 27001 or ISO/IEC 20000-1. Equally, it does not describe all parts of each International Standard comprehensively. Only those parts where subject matter overlaps or differs are described in detail. It is assumed that users of this document have access to ISO/IEC 20000-1 and ISO/IEC 27001.

NOTE Specific legislations can exist, which can impact the planning of an organization's management system.

Information security, cybersecurity and privacy protection — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

1 Scope

This document gives guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for organizations intending to:

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 document 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.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 20000-1:2018, *Information technology — Service management — Part 1: Service management system requirements*

ISO/IEC 27000:2018, *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 and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27000:2018 and ISO/IEC 20000-1:2018 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

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

4.1 Understanding ISO/IEC 27001 and ISO/IEC 20000-1

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. Subclauses 4.2 to 4.4 provide an introduction to the main concepts underlying ISO/IEC 27001 and ISO/IEC 20000-1 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 information security management system (ISMS) to protect information. Information can take any form, be stored in any way 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. As part of a risk treatment process, the organization should select, implement, monitor and review a variety of measures to manage identified risks. These measures are known as information security 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. Excluding any of the requirements specified in ISO/IEC 27001:2013, Clauses 4 to 10, is not acceptable when an organization claims conformity to ISO/IEC 27001.

4.3 ISO/IEC 20000-1 concepts

ISO/IEC 20000-1 specifies requirements for establishing, implementing, maintaining and continually improving a service management system (SMS). An SMS supports the management of the service lifecycle, including the planning, design, transition, delivery and improvement of services, which meet agreed requirements and deliver value for customers, users and the organization delivering the services.

Some of the requirements specified in ISO/IEC 20000-1 are grouped into clauses indicating processes, such as incident management, change management and supplier management. Some requirements for information security management are specified in ISO/IEC 20000-1:2018, 8.7.3. All requirements specified in ISO/IEC 20000-1 are generic and are intended to be applicable to all organizations, regardless of the organization's type or size, or the nature of the services delivered. ISO/IEC 20000-1 is intended for management of services using technology and digital information. Exclusion of any of the requirements in ISO/IEC 20000-1:2018, Clauses 4 to 10, is not acceptable when the organization claims conformity to ISO/IEC 20000-1, irrespective of the nature of the organization.

4.4 Similarities and differences

Service management and information security management are sometimes treated as if they are neither connected nor interdependent. The context for such separation is that service management can easily be related to efficiency, service quality, customer satisfaction 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. There are some shared concepts between these two disciplines, as well as concepts that are unique to each.

Information security management and service management clearly address very similar requirements and activities, even though the SMS and the ISMS each highlight different details. When working with ISO/IEC 27001 and ISO/IEC 20000-1, it should be understood that their characteristics differ in more than one aspect. It is possible that the scopes of an ISMS and an SMS can differ (see 5.2). They also have different intended outcomes. 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 recover from or prevent information security incidents.

See Annex A for details of the correspondence between ISO/IEC 27001:2013, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10. See Annex B for a comparison of topics between the controls in ISO/IEC 27001:2013, Annex A, and the requirements in ISO/IEC 20000-1:2018. See Annex C for a comparison of terms and definitions between ISO/IEC 27000 and ISO/IEC 20000-1.

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:

— unofficial management arrangements exist which cover both information security management and service management but have not been formalized, documented or deliberately integrated into the organization's other activities;

— there is a management system based on ISO/IEC 27001 or ISO/IEC 20000-1;

— there are separate management systems based on ISO/IEC 27001 and ISO/IEC 20000-1, 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) the scope(s) of the proposed ISMS and SMS, as well as any difference in scope between them, if applicable;

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

d) elements of each management system which can be integrated and how they can be integrated;

e) elements that are to remain separate;

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

g) the impact on technology in use;

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

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

j) education and training in the integrated management system;

k) accountabilities and responsibilities for all requirements;

l) phases and sequence of implementation activities.

5.2 Considerations of scope

One area where an ISMS and an SMS can differ is on the subject of scope, namely, what assets, services, processes and parts of the organization the management system should include.

ISO/IEC 20000-1 is concerned with the planning, design, transition, delivery and improvement of services to deliver value to customers, users and the organization. The scope of ISO/IEC 20000-1 includes those activities that deliver services. The scope of an SMS can include all or some of the services delivered by the organization. The organization in the scope of the SMS can be a whole or part of a larger entity. The SMS scope can also be defined exclusively by a clear physical boundary, such as a single site delivering services. The organization in the scope of the SMS can also be known as a service provider.

ISO/IEC 27001 is concerned with how to manage information security risk. The scope of the ISMS covers those activities related to managing the confidentiality, integrity and availability of the organization's information.

For ISO/IEC 27001, the definition of the organization is that which is covered by the ISMS. As with an SMS, an ISMS can be applied to part or all of an entity and can include services delivered by the organization. The ISMS scope can also be defined exclusively by a clear physical boundary, such as a security perimeter around a specific site or part of a site.

In some cases, the full requirements specified in ISO/IEC 20000-1 and ISO/IEC 27001 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 other parties provide or operate all the services, service components or processes in the scope of the SMS. ISO/IEC 20000-1:2018, 8.2.3, states that not all services, service components and processes can be provided by other parties – the organization itself should provide at least some of these.

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 20000-1 and ISO/IEC 27001, the integrated management system should take both ISO/IEC 20000-1 and ISO/IEC 27001 into consideration (see Annex A). Differences in scope can result in some services included in the SMS being excluded from the scope of 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 but not in the ISMS. 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 and to maximize the benefits of the integrated management system.

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. Subclauses 5.3.2, 5.3.3 and 5.3.4 provide suggestions for implementation in each of the three states 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 an ISMS or an SMS 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 have some form of management system, which may simply be its processes, plans and policies. This should be adapted to achieve conformity with the requirements specified in either ISO/IEC 27001 and ISO/IEC 20000-1, or both.

The decision regarding the order in which the requirements for the ISMS and the SMS will be implemented should be based on business needs and priorities. Decisions can be influenced by the primary driver, for example, competitive positioning or the need to demonstrate conformity to a customer or other interested party.

Another important decision is whether to implement both an SMS and an ISMS concurrently or sequentially. If the implementation is sequential, either the SMS or the ISMS is implemented and then that management system is extended to include the additional requirements of the other. Both an SMS and an ISMS can be implemented concurrently, if implementation activities and efforts can be coordinated and duplication minimized. However, depending on the nature of the organization, it can be prudent to start with the requirements specified in one standard and then expand the management system to include the requirements of the other.

These considerations are illustrated in the following scenarios.

— Scenario 1: 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 the requirements specified in ISO/IEC 27001.

— Scenario 2: An organization that is using other parties for delivery of some services or parts of a service should initially focus on ISO/IEC 20000-1. ISO/IEC 20000-1 includes more requirements for managing other parties, including external and internal suppliers as well as customers acting as a supplier. The organization should then proceed to ISO/IEC 27001.

— Scenario 3: A small organization should focus on one of either ISO/IEC 27001 or ISO/IEC 20000-1, depending on its level of reliance on service management or information security.

— Scenario 4: An organization can choose to implement an ISMS and SMS concurrently. This can be handled as a single project, or as two parallel sub-projects within one overarching programme of work that includes a third sub-project focused on the integration.

— Scenario 5: 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.

An integration working group holding regular meetings during the implementation of requirements for both an SMS and an ISMS can help in ensuring better alignment and integration, as well as minimizing duplication of effort.

5.3.3 The management system fulfils the requirements of one of the standards

Where the organization's management system has already achieved conformity with the requirements specified in ISO/IEC 20000-1 or ISO/IEC 27001, the primary goal should be to integrate the requirements of the other standard. This should be done without suffering any loss of service or jeopardizing information security. This should be carefully planned in advance, with existing documentation being reviewed by a team with a good understanding of both the standards.

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

a) scope;

b) management system structure;

c) policies;

d) planning activities;

e) authorities and responsibilities;

f) practices;

g) relevant processes;

h) procedures;

i) risk management methodologies;

j) terms and definitions;

k) resources.

These attributes should then be reviewed to establish how they can be applied to the integrated management system.

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 of the management systems as described in 5.2.

There are three potential scenarios:

— Scenario 1: the scope of the ISMS and SMS are identical;

— Scenario 2: the scope of the ISMS and SMS are overlapping but not identical;

— Scenario 3: the scope of the ISMS and the SMS are different.

It is not necessary to have identical boundaries of scope but the greatest benefit from the integration can come from an identical or significantly overlapping scope.

Even where an ISMS and an SMS have different scopes, the organization should seek to integrate the common requirements for all management system standards, which include those for internal audit, management review and continual improvement.

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 relevant interested parties of both management systems with one another;

e) plan the most appropriate 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 while maintaining conformity, an extensive planning phase should be completed.

6 Integrated implementation considerations

6.1 General

Both ISO/IEC 27001 and ISO/IEC 20000-1 now use the same clause structure, common terms and common requirements, which is known as the harmonized structure for management system standards. This common structure, as well as the common requirements and terms, facilitates the integration of an ISMS and an SMS.

An integrated management system should use consistent and clear terminology. This can result in expressing requirements from one or both of the standards differently from the wording of the published version(s). However, the organization should still ensure clear traceability to the requirements specified in both ISO/IEC 27001 and ISO/IEC 20000-1.

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 and authorities can be created for the integrated management system. To support this, the organization can create a traceability matrix to explicitly show 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.

In all cases, the organization's goal should be to produce a viable integrated management system that enables conformity to the requirements specified in ISO/IEC 27001 and ISO/IEC 20000-1. The goal is not to compare the standards or to determine which is best or right. Where there is conflict between viewpoints within the organization, this should be resolved in a way which satisfies the requirements specified in ISO/IEC 27001 and ISO/IEC 20000-1 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, 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 ISO/IEC 27001 and ISO/IEC 20000-1.

6.2 Potential challenges

6.2.1 Requirements and controls

ISO/IEC 27001:2013, Clauses 4 to 10, specifies requirements for an ISMS. In addition, ISO/IEC 27001:2013, Annex A, contains an extensive list of control objectives and controls. The controls in ISO/IEC 27001:2013, Annex A, are not requirements and are not mandatory. ISO/IEC 27001:2013, 6.1.3, specifies that the organization determine all controls necessary to implement information security risk treatment options chosen and then compare these controls with those in ISO/IEC 27001:2013, Annex A, to verify that no necessary controls have been omitted. The statement of applicability (SoA) is then used to record which controls are relevant to the organization's ISMS. Control objectives are implicitly included in the controls selected. The control objectives and controls listed in ISO/IEC 27001:2013, Annex A, are not exhaustive and can be substituted with others, or additional control objectives and controls can be added as needed. This means it is possible to include only a subset of the controls in ISO/IEC 27001:2013, Annex A, or indeed to not include any of the ISO/IEC 27001:2013, Annex A, controls in the organization's SoA. Any control within ISO/IEC 27001:2013, Annex A, that does not contribute to modifying risk in a cost-effective manner is not necessary. Similarly, controls not included in ISO/IEC 27001:2013, Annex A, can be determined as necessary to modify risk.

ISO/IEC 20000-1 specifies requirements for an SMS but does not list any controls and does not specify a requirement for an SoA, so there is no direct correlation between ISO/IEC 27001:2013, Annex A, and ISO/IEC 20000-1. However, ISO/IEC 20000-1:2018, 8.7.3.2, does include requirements to determine controls to address information security risks to the SMS and the services, and to document the decisions about these controls. In addition, there is a requirement to monitor and review the effectiveness of these controls, taking action if required.

Organizations wishing to integrate an ISMS and an SMS need to distinguish between the requirements specified in ISO/IEC 27001 and ISO/IEC 20000-1, and the information security controls specified in ISO/IEC 27001:2013, Annex A. Even if it appears that there is a common topic area between a requirement specified in ISO/IEC 20000-1 and a control included in ISO/IEC 27001:2013, Annex A, the distinction between requirements and controls needs to be understood and communicated to avoid confusion within the organization.

Annex B of this document provides a comparison of topics between the requirements specified in ISO/IEC 20000-1 and the controls in ISO/IEC 27001:2013, Annex A.

6.2.2 Assets and configuration items

In ISO/IEC 27001 and ISO/IEC 20000-1, there are both differences and similarities in the usage and meaning of asset.

ISO/IEC 20000-1 uses the definition of asset from ISO/IEC 19770-5 which is "item, thing or entity that has potential or actual value to an organization". The single requirement for asset management in ISO/IEC 20000-1 is minimal to ensure that assets used to deliver services are managed to meet service requirements and obligations such as legal and regulatory requirements.

Asset is not a defined term in ISO/IEC 27001, so it is used in its normal English language sense of something of value. ISO/IEC 27000:2018, 4.2.2, explains that "information is an asset that, like other important business assets, is essential to an organization's business and, consequently, needs to be suitably protected". ISO/IEC 27001:2013, Annex A, includes asset management as a control.

ISO/IEC 27001 is focused on the management of risks impacting all information within the 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 holding or handling information, can also be assets. For example, a data cable can be an asset. Although it is not information, the cable is the resource used for carrying information and therefore is relevant to risk assessment in ISO/IEC 27001.

Information is also seen as a resource in ISO/IEC 20000-1. For example, ISO/IEC 20000-1:2018, 7.1, specifies that the human, technical, financial and information resources needed for the SMS and the services are determined.

Neither of the standards requires every asset 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 ISO/IEC 27001 and ISO/IEC 20000-1. At the beginning of any integration work, a decision should be made on the way in which assets will be classified, categorized and identified. This is to ensure that unambiguous references can be made to assets.

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". Some assets contributing to a service are also CIs subject to configuration management, as specified in ISO/IEC 20000-1:2018, 8.2.6. For example, a service monitoring application or a server are assets that are likely to be CIs, because they are critical to delivering the service and need to be controlled. If the term asset is used to refer to information, specific assets can be given an additional classification if their status is also recognized as a CI in ISO/IEC 20000-1

The concept of configuration information in ISO/IEC 20000-1 is similar to the asset inventory in ISO/IEC 27001 but perspectives differ.

The configuration management requirements in ISO/IEC 20000-1:2018, 8.2.6, can be used to support the classification and management of information in the scope of an ISMS. From the ISO/IEC 27001 perspective, the organization should manage the security of the configuration information, including availability, integrity and confidentiality. Configuration baselines can include content with security implications and the confidentiality, integrity and availability of this information should be considered when integrating an ISMS and SMS.

6.2.3 Service design and transition

ISO/IEC 20000-1:2018, 8.5.2, includes requirements for service design and transition. There are no directly equivalent requirements in ISO/IEC 27001, although several aspects of service design, transition and delivery are covered in controls listed in ISO/IEC 27001:2013, Annex A.

An integrated management system should ensure that information security is considered in detail during the planning, design and transition to operations for all new or changed services. Topics that should be considered include an assessment of the impact of the new or changed service on existing information security controls. This should be done regardless of whether the service falls within the scope of the ISMS. It should also be done for the removal of a service.

6.2.4 Risk assessment and management

Even though risks are considered as part of both an ISMS and an SMS, the nature of some of these risks can differ. 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 in the scope of an SMS, e.g. the risk of an organization not meeting its service targets for customer satisfaction, would not be considered as risks from the perspective of an ISMS. However, risks related to not meeting service requirements can be relevant to both the ISMS and the SMS if any of the service requirements involve information security. Risks identified within the scope of the SMS cannot be assumed to be relevant to the ISMS, and vice versa, but they should be considered in terms of both. Examples of risks that should be considered from both the service management and information security management perspectives include, but are not limited to, risks during the planning of services, risks related to changes, risks to service availability and risks to business continuity.

The ownership of risk can also differ between the two disciplines. Within the scope of the SMS, risk ownership is not a mandatory requirement. For an SMS, ownership can be with the organization, a customer, suppliers, or other parties. For example, a customer can potentially be expected to approve some residual risks as part of their SLA or the service continuity plan. In ISO/IEC 27001:2013, 6.1.2, there is a requirement specified for identification of a risk owner but the matter of risk ownership as internal or external to the organization is not specified. In practice the organization is considered the owner of all information security risks in the scope of the ISMS.

ISO/IEC 27001:2013, 6.1, and ISO/IEC 27001:2013, Clause 8, specify requirements for assessing and treating aspects of risk associated with information security. These requirements specify both management of risks to the effectiveness of the ISMS and the risks to the information in the scope of the ISMS. ISO/IEC 27001:2013, 6.1, provides detail on how to carry out information security risk assessment and treatment.

ISO/IEC 20000-1:2018, 6.1, specifies requirements to determine and document risks to the SMS and the services. This includes risks to the organization, as well as risks related to not meeting service requirements and the involvement of other parties in the service lifecycle. These categories of risk can also be used, when implementing an ISMS, for the categorization of information security risks.

Risk evaluation can have a different focus depending on the different perspectives of information security management and service management. When planning the integrated implementation, organizations should be mindful of any differences in risk criteria and the impact that these differences will have on risk evaluation.

The organization should adopt one of these described approaches.

a) Use one common approach to risk management, including risk assessment avoiding duplication. For example, the risk of loss of availability of an information asset can be shared by the different parts of the integrated management system.

b) Use separate risk assessment approaches for ISO/IEC 20000-1 and ISO/IEC 27001. If this option is chosen, the organization should use terminology that differentiates risk assessment of the SMS and services from the 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 or service management.

Whatever approach is taken, subdividing risk assessment and treatment to separately consider risks that affect both information security and service management, from risks that affect one but not both perspectives, 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 more explicit and detailed risk assessment and risk treatment requirements.

6.2.5 Risk and other parties

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:

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 can differ from the level of security that the third party considers to be sufficient;

b) the organization retains some information about the third party, e.g. the third party's own financial records in the scope of the organization's ISMS. 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.

Both ISO/IEC 20000-1 and ISO/IEC 27001 specify requirements for risk acceptance criteria to be defined but these criteria can differ between an information security and a service management perspective.

6.2.6 Incident management

The first point of comparison regarding incident management between ISO/IEC 20000-1 and ISO/IEC 27001 is that of terminology. In ISO/IEC 27000, the defined term for an event which has a significant impact on information security is an information security incident. In contrast, in ISO/IEC 20000-1, there are several specialized terms linked with incident management. For example, incident, major incident, information security incident, problem, known error. 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 for resolution, such as incident 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. Figure 1 illustrates the relationship between information security incident management in ISO/IEC 27001 and incident management in ISO/IEC 20000-1. In Figure 1, incidents from ISO/IEC 20000-1 have been referred to as "service incidents" to distinguish them from information security incidents in ISO/IEC 27001.

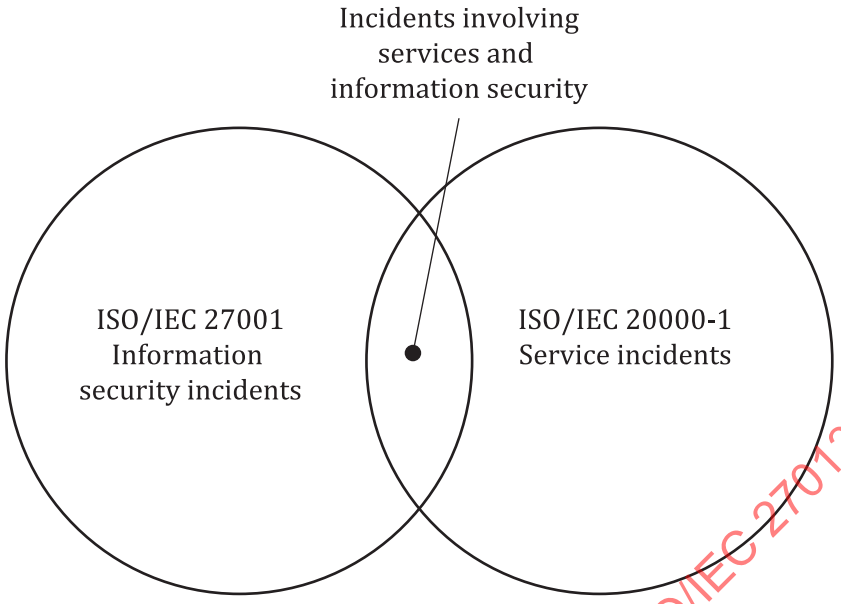

Figure 1 — Illustration of relationship between standards for the management of incidents

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

EXAMPLE 1 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.

EXAMPLE 2 The lock for the door to a customer's office is found to be broken. This event can be considered an information security incident under ISO/IEC 27001. However, this would not fall within the scope of ISO/IEC 20000-1 unless the event impacted information relevant to the requirements in ISO/IEC 20000-1:2018, 8.7.3, 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.

EXAMPLE 3 Scheduled maintenance exceeds SLA limits.

EXAMPLE 4 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 availability of information 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 the ISMS and SMS.

ISO/IEC 27001 and ISO/IEC 20000-1 both require the organization to analyse data and trends on incidents.

Defining and publishing criteria to help regular operations or service desk personnel determine whether an incident should be classified as an information security incident can facilitate more consistent and effective classification.

6.2.7 Problem management

Problem management is the process in ISO/IEC 20000-1 for identifying the root cause of one or more actual or potential incidents to minimize or avoid the impact of incidents. In ISO/IEC 27001, the term problem management is not used, but information security incidents can be analysed to identify patterns

and potential causes that need to be addressed. ISO/IEC 27001:2013, 10.1, and ISO/IEC 20000-1:2018, 10.1, include the concept of identifying patterns of nonconformities and addressing them.

ISO/IEC 27001 uses multiple inputs to risk analysis. In an integrated management system, these can include identified problems and known errors from the problem management process. Equally, the problem management process can utilize information provided by the information security incident management process.

In an integrated management system, the scope of the problem management process should be defined. If an ISMS is implemented before the SMS, it can be useful to integrate the requirements specified in ISO/IEC 20000-1 for problem management as part of the ISMS due to its benefits for all management systems.

6.2.8 Gathering of evidence

Another point of comparison and consideration 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 an information security incident is investigated in order to understand the cause. It is important that the organization consider the balance between the service management mindset which is focused on restoring service as quickly as possible following an incident, and the information security mindset, which is focused on preserving evidence and potentially observing the incident in progress to gather information. Care should be taken, when integrating an SMS and an ISMS, to ensure conformance to all requirements for managing information security incidents. For example, information security controls can include the collection, retention and provision of evidence for disciplinary or legal purposes.

It should be recognized that, in the case of an information security incident, the requirement to collect evidence can mean that the affected service cannot be restored within agreed service targets. ISO/IEC 20000-1 specifies a requirement to prioritize, taking into consideration the information security risk related to the incident. 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.

This can mean that additional time is required to collect evidence before an information security incident is resolved.

6.2.9 Major incident management

In some cases, an information security incident can be a major incident, based on the requirements for major incidents specified in ISO/IEC 20000-1:2018, 8.6.1. According to the major incident management requirements in ISO/IEC 20000-1, top management are kept informed of all major incidents. This includes those that are also information security incidents. Top management should ensure that those investigating information security incidents have appropriate skills and that parties involved in collecting and analysing evidence are suitably experienced.

A major incident should not necessitate a delay in resolution for the collection of evidence in the case of an information security incident. For example, if a website handling customer payment is found to have been compromised and payment details taken, this would be a major incident and an information security incident where gathering evidence would be vital. Evidence collection and service restoration times should be adequately covered in service requirements and in service level agreements (SLAs).

6.2.10 Classification and escalation of incidents

The organization should determine the criteria it uses to classify incidents according to its requirements for special treatment, e.g. where an incident has heightened requirements for confidentiality. In these cases, the organization should establish a process whereby an incident is either handed over to specialist information security personnel or coordinated in parallel by service incident management personnel and information security personnel.

Some information security incidents should not be handled using the incident management or major incident procedure, but by the information security management function. The organization's procedures can identify the criteria for determining when an incident should be transferred to the information security function. An example of such an incident can be an internal breach of security which requires police investigation and forensic examination. These types of incidents require visibility and even awareness of their existence to be limited to a smaller group than would normally be the case. The skills needed to investigate an information security incident are often different than those needed to investigate other incident types.

Due to the sensitivity of the information in some information security incident records, the ability to access or update details of these incidents should only be available to personnel with appropriate security clearance or authorization.

6.2.11 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, requires the organization to control planned changes. ISO/IEC 27001:2013, Annex A, also includes control objectives and controls related to change management.

ISO/IEC 20000-1:2018, 8.5.1, includes extensive requirements for change management which can be adopted by an ISMS. ISO/IEC 20000-1:2018, 8.5.1.3, includes requirements for decision making about changes to consider potential risks and impacts of the change on information security.

To ensure that change management requirements are fulfilled, tasks and supporting checklists for impact assessment or post-implementation review can be developed as part of the integrated management system based on the requirements specified in ISO/IEC 20000-1. This should ensure that all relevant information security risks are reviewed as part of the change management process.

6.3 Potential gains

6.3.1 Service level management and reporting

ISO/IEC 20000-1:2018, 9.4, specifies requirements for the organization to determine reporting requirements and their purpose. Service reports can be beneficial to maintaining and improving information security. For example, reporting on information security incidents and their impact on service level targets.

When implementing an ISMS, 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 requirements specified in ISO/IEC 20000-1:2018, 9.4, so that relevant and timely information can be used to maintain or improve information security. Where appropriate, 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 information security 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.

6.3.2 Management commitment and continual improvement

Top management commitment is required to make both the SMS and the ISMS effective. ISO/IEC 20000-1 includes a requirement for top management to ensure that what constitutes value for the organization and its customers be determined. It is also important that the value of an ISMS is understood by the organization.

ISO/IEC 27001 describes information security in relation to "interested parties". These are parties with a specific interest in the organization in the scope of the ISMS and should be considered when

defining the value of the ISMS. These parties can include staff, shareholders, customers and in some cases regulatory authorities or the general public.

ISO/IEC 20000-1 refers to customers and other interested parties. Interested parties are a person or group having a specific interest in the performance or success of the organization's SMS or services. Therefore, "interested parties", as used in ISO/IEC 20000-1, is similar to "interested parties" as used in ISO/IEC 27001.

Both ISO/IEC 27001:2013, 5.1, and ISO/IEC 20000-1:2018, 5.1, specify requirements for top management to promote continual improvement, while ISO/IEC 27001:2013, 5.2, and ISO/IEC 20000-1:2018, 5.2, require top management to establish a policy which includes a commitment to continual improvement. ISO/IEC 20000-1 specifies that this commitment is for both the SMS and the services.

Both ISO/IEC 27001:2013, 10.2, and ISO/IEC 20000-1:2018, 10.2, refer to the organization managing various aspects of continual improvement, stating that the organization carry out continual improvement of its management system. ISO/IEC 20000-1 specifies that this is for the services as well as the SMS.

ISO/IEC 20000-1:2018, 10.2, specifies requirements for evaluation criteria to be applied to opportunities for improvement and includes the alignment of improvements with service management objectives. ISO/IEC 20000-1:2018, 10.2, also specifies requirements for the organization to manage, measure and report on improvements to the SMS and services. The ISMS can find these additional requirements of the SMS for improvement useful.

6.3.3 Capacity management

There are requirements specified in ISO/IEC 27001:2013, 7.1, and ISO/IEC 20000-1:2018, 7.1, for determining and providing resources, which is closely related to capacity management.

Capacity management in ISO/IEC 20000-1:2018, 8.4.3, includes a wide range of capacity concepts. For example, capacity management as specified in ISO/IEC 20000-1 applies to human, technical, information and financial resources. There is no specific requirement for capacity management in ISO/IEC 27001, but where an organization has selected relevant controls to address capacity-related risks, a focus across these four types of capacity resources can be beneficial.

ISO/IEC 20000-1:2018, 8.4.2, specifies requirements for demand management. It can be useful to understand the current and forecast future demand for services to ensure that information security controls can support the demand.

In ISO/IEC 27000:2018, 3.7, availability is defined to mean both accessible and usable. Capacity management in ISO/IEC 20000-1:2018, 8.4.3, 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. due to limited network capacity.

6.3.4 Management of third parties and related risk

In ISO/IEC 27001, a third party, such as an external customer or supplier, can affect the activities of the ISMS and can be a potential source of risk. ISO/IEC 27001:2013, 8.1, and ISO/IEC 20000-1:2018, 8.1, both specify a requirement that the organization ensure that outsourced processes are determined and controlled. ISO/IEC 27001:2013, Annex A, includes controls related to supplier relationships.

ISO/IEC 20000-1 specifies that other parties are entities not under the direct control of the organization in the scope of the SMS, but can contribute to the services or service management activities in the scope of the SMS. Other parties can include external suppliers, internal suppliers or customers acting as a supplier. Other parties can contribute to a major part of the service (see ISO/IEC 20000-1:2018, 8.2.3).

ISO/IEC 20000-1:2018, 8.7.3, specifies requirements for information security management. This includes the management of risk associated with external organizations, which can directly affect the customer organization's information security. ISO/IEC 20000-1 specifies other requirements

which support the management of third-party risk. These are ISO/IEC 20000-1:2018, 8.3.4, supplier management and ISO/IEC 20000-1:2018, 8.2.3, control of parties involved in the service lifecycle.

When designing an integrated management system, there are two main considerations which affect the supplier management practices in regard to managing third party risks.

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 organization to consider risks associated with other parties.

b) Information security should be considered where other parties are involved with the design, build, test, deployment or operation of a new or changed service. This should also be considered as part of any agreements relevant to those other parties.

Other concepts covered in ISO/IEC 20000-1:2018, 8.3.2, business relationship management, 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.

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 or other documented agreements. This approach should ensure that the other party applies appropriate controls.

ISO/IEC 27001:2013, Annex A, includes controls related to supplier management. It also references employees and contractors across multiple controls.

ISO/IEC 20000-1 risk assessments can be extended, using requirements specified in ISO/IEC 27001, 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.

6.3.5 Continuity and availability management

ISO/IEC 20000-1:2018, 8.7.1, and ISO/IEC 20000-1:2018, 8.7.2, explicitly cover two areas of interest for information security: service availability management and service continuity management. However, requirements for service availability management and service continuity management in ISO/IEC 20000-1 do not include specific requirements for integrity and confidentiality, so activities within an existing management system should be reviewed to see if they can usefully be extended to cover integrity and confidentiality. It is also important to note that the ISO/IEC 27000 definition of availability differs from the ISO/IEC 20000-1 definition of service availability and that service continuity is a subset of business continuity.

An organization looking to integrate an SMS and an ISMS should be careful to understand both the differences and the opportunities for mutual support between service management and information security management when assessing and applying the concepts of continuity and availability.

ISO/IEC 27001:2013, Annex A, includes controls which concern how to manage information security during an adverse situation when the business continuity plan needs to be invoked. ISO/IEC 27001:2013, Annex A, also includes controls related to availability.

6.3.6 Release and deployment management

Requirements specified for release and deployment management in ISO/IEC 20000-1:2018, 8.5.3, should include relevant information security considerations. If information security is not considered in release and deployment management, issues can arise. For example, changes can be made to the operation of live system(s) which introduce information security vulnerabilities if release and deployment management does not take into account the possibility of malicious action.

This is particularly important during emergency releases. In these situations, different release and deployment management procedures can be used, due to time and/or resource constraints, where some activities are performed after the deployment. The risks of compromising information security can therefore be increased.

Release and deployment management can be improved through the selection of relevant controls, such as those in ISO/IEC 27001:2013, Annex A.

Annex A
(informative)

Correspondence between ISO/IEC 27001:2013, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10

Table A.1 provides a comparison of content at a clause level between ISO/IEC 27001:2013, Clauses 1 to 10, and ISO/IEC 20000-1:2018, Clauses 1 to 10.

Clauses where there is overlap in most of the requirements and details between ISO/IEC 27001 and ISO/IEC 20000-1 are highlighted in grey. Those with grey highlight are not necessarily exactly the same but have significant correlations, due to the harmonized structure for management system standards. The bold text in the table is for clause or subclause headings which themselves contain no text or requirements.

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

ISO/IEC 27001:2013	ISO/IEC 20000-1:2018
Introduction – specific to each standard	Introduction
1 Scope – specific to each standard	**1 Scope** 1.1 General 1.2 Application
2 Normative references – specific to each standard	2 Normative references
3 Terms and definitions – specific to each standard	3 Terms and definitions
4 Context of the organization	**4 Context of the organization**
4.1 Understanding the organization and its context	4.1 Understanding the organization and its context
4.2 Understanding the needs and expectations of interested parties	4.2 Understanding the needs and expectations of interested parties
4.3 Determining the scope of the information security management system	4.3 Determining the scope of the service management system
4.4 Information security management system	4.4 Service management system
5 Leadership	**5 Leadership**
5.1 Leadership and commitment	5.1 Leadership and commitment
5.2 Policy	**5.2 Policy** 5.2.1 Establishing the service management policy 5.2.2 Communicating the service management policy 8.7.3.1 Information security policy
5.3 Organizational roles, responsibilities and authorities	5.3 Organizational roles, responsibilities and authorities

Table A.1 *(continued)*

ISO/IEC 27001:2013	ISO/IEC 20000-1:2018
6 Planning	**6 Planning**
6.1 Actions to address risks and opportunities	**6.1 Actions to address risks and opportunities**
6.1.1 Actions to address risks and opportunities – General	6.1.1 6.1.3 Other risk references: 6.1.2 6.3 Plan the SMS 8.2.2 Plan the services 8.3.4.1 Management of external suppliers 8.5.1.3 Change management activities 8.7.1 Service availability management 8.7.2 Service continuity management 8.7.3 Information security management 9.3 Management review 10.2 Continual improvement
6.1.2 Information security risk assessment	8.7.3.2 Information security controls
6.1.3 Information security risk treatment	8.7.3.2 Information security controls
6.2 Information security objectives and planning to achieve them	**6.2 Service management objectives and planning to achieve them** 6.2.1 Establish objectives 6.2.2 Plan to achieve objectives
7 Support	**7 Support of the service management system**
7.1 Resources	7.1 Resources
7.2 Competence	7.2 Competence
7.3 Awareness	7.3 Awareness
7.4 Communication	7.4 Communication
7.5 Documented information 7.5.1 General 7.5.2 Creating and updating 7.5.3 Control of documented information	**7.5 Documented information** 7.5.1 General 7.5.2 Creating and updating documented information 7.5.3 Control of documented information
8 Operation	**8 Operation of the service management system**
8.1 Operational planning and control	8.1 Operational planning and control
8.2 Information security risk assessment	8.7.3.2 Information security controls
8.3 Information security risk treatment	8.7.3.2 Information security controls
9 Performance evaluation	**9 Performance evaluation**
9.1 Monitoring, measurement, analysis and evaluation	9.1 Monitoring, measurement, analysis and evaluation
9.2 Internal audit	9.2 Internal audit
9.3 Management review	9.3 Management review
10 Improvement	**10 Improvement**
10.1 Nonconformity and corrective action	10.1 Nonconformity and corrective action
10.2 Continual improvement	10.2 Continual improvement

Annex B
(informative)

Correspondence between the controls in ISO/IEC 27001:2013, Annex A, and the requirements in ISO/IEC 20000-1:2018, Clauses 4 to 10

Table B.1 provides a comparison of topics between the controls in ISO/IEC 27001:2013, Annex A, and the requirement of ISO/IEC 20000-1:2018, Clauses 4 to 10.

ISO/IEC 27001:2013, Annex A, contains a list of control objectives and controls. The controls in ISO/IEC 27001:2013, Annex A, are not requirements and are not mandatory. ISO/IEC 27001:2013, 6.1.3, specifies that the organization determine all controls necessary to implement information security risk treatment options chosen and then compare these controls with those in ISO/IEC 27001:2013, Annex A, to verify that no necessary controls have been omitted. The statement of applicability (SoA) is then used to record which controls are relevant to the organization's ISMS. Control objectives are implicitly included in the controls selected. The control objectives and controls listed in ISO/IEC 27001:2013, Annex A, are not exhaustive and can be substituted with others, or additional control objectives and controls can be added as needed. This means it is possible for the organization's SoA to:

a) include only a subset of the controls in ISO/IEC 27001:2013, Annex A;

b) not include any of the ISO/IEC 27001:2013, Annex A, controls;

c) include alternative controls;

d) include a combination of controls from ISO/IEC 27001:2013, Annex A, and other sources.

Any control within ISO/IEC 27001:2013, Annex A, that does not contribute to modifying risk in a cost-effective manner is not necessary. Similarly, controls not included in ISO/IEC 27001:2013, Annex A, can be determined as necessary to modify risk.

ISO/IEC 20000-1 specifies requirements for the SMS but does not list any controls and does not specify a requirement for an SoA, so there is no direct correlation between ISO/IEC 27001:2013, Annex A, and ISO/IEC 20000-1. However, ISO/IEC 20000-1:2018, 8.7.3.2, includes a requirement to determine controls to address information security risks to the SMS and the services, and to document the decisions about these controls. In addition, there is a requirement to monitor and review the effectiveness of these controls, taking action if required.

Organizations wishing to integrate an ISMS and an SMS need to distinguish between the requirements specified in ISO/IEC 27001 and ISO/IEC 20000-1, and the information security controls specified in ISO/IEC 27001:2013, Annex A. Even if it appears that there is a common topic area between a requirement specified in ISO/IEC 20000-1 and a control included in ISO/IEC 27001:2013, Annex A, the distinction between requirements and controls needs to be understood and communicated to avoid confusion within the organization.

Where there is overlap in a topic between controls in ISO/IEC 27001:2013, Annex A, and ISO/IEC 20000-1:2018, Clauses 1 to 10, they are highlighted in grey. Those with grey highlight have significant correlations. Areas with no shading are those where there is little or no overlap in topic.

Table B.1 — Correspondence between ISO/IEC 27001:2013, Annex A, and ISO/IEC 20000-1:2018

ISO/IEC 27001:2013, Annex A	ISO/IEC 20000-1:2018
A.5 Information security policies	
A.5.1 Management direction for information security	8.7.3.1 Information security policy
A.6 Organization of information security	
A.6.1 Internal organization	Not specified in ISO/IEC 20000-1
A.6.2 Mobile devices and teleworking	Not specified in ISO/IEC 20000-1
A.7 Human resource security	
A.7.1 Prior to employment	Not specified in ISO/IEC 20000-1
A.7.2 During employment	Not specified in ISO/IEC 20000-1
A.7.3 Termination and change of employment	Not specified in ISO/IEC 20000-1
A.8 Asset management	
A.8.1 Responsibility for assets	8.2.5 Asset management
A.8.2 Information classification	Not specified in ISO/IEC 20000-1
A.8.3 Media handling	Not specified in ISO/IEC 20000-1
A.9 Access control	
A.9.1 Business requirements of access control	Not specified in ISO/IEC 20000-1
A.9.2 User access management	8.6.2 Service request management
A.9.3 User responsibilities	Not specified in ISO/IEC 20000-1
A.9.4 System and application access control	Not specified in ISO/IEC 20000-1
A.10 Cryptography	
A.10.1 Cryptographic controls	Not specified in ISO/IEC 20000-1
A.11 Physical and environmental security	
A.11.1 Secure areas	Not specified in ISO/IEC 20000-1
A.11.2 Equipment	Not specified in ISO/IEC 20000-1
A.12 Operations security	
A.12.1 Operational procedures and responsibilities	8.4.3 Capacity management 8.5.1 Change management 8.5.2 Service design and transition
A.12.2 Protection from malware	Not specified in ISO/IEC 20000-1
A.12.3 Backup	Not specified in ISO/IEC 20000-1
A.12.4 Logging and monitoring	Not specified in ISO/IEC 20000-1
A.12.5 Control of operational software	Not specified in ISO/IEC 20000-1
A.12.6 Technical vulnerability management	Not specified in ISO/IEC 20000-1
A.12.7 Information systems audit considerations	Not specified in ISO/IEC 20000-1
A.13 Communications security	
A.13.1 Network security management	Not specified in ISO/IEC 20000-1
A.13.2 Information transfer	Not specified in ISO/IEC 20000-1
A.14 System acquisition, development and maintenance	
A.14.1 Security requirements of information systems	8.5.2 Service design and transition
A.14.2 Security in development and support processes	8.2.3 Control of parties involved in the service lifecycle 8.5.1 Change management 8.5.2 Service design and transition 8.5.3 Release and deployment management

Table B.1 *(continued)*

ISO/IEC 27001:2013, Annex A	ISO/IEC 20000-1:2018
A.14.3 Test data	Not specified in ISO/IEC 20000-1
A.15 Supplier relationships	
A.15.1 Information security in supplier relationships	8.2.3 Control of parties involved in the service lifecycle 8.3.4 Supplier management 8.7.3.2 Information security controls
A.15.2 Supplier service delivery management	8.3.4 Supplier management 8.5.1 Change management
A.16 Information security incident management	
A.16.1 Management of information security incidents and improvements	8.6.1 Incident management 8.6.3 Problem management 8.7.3.3 Information security incidents
A.17 Information security aspects of business continuity management	
A.17.1 Information security continuity	8.7.2 Service continuity management
A.17.2 Redundancies	8.7.1 Service availability management 8.7.2 Service continuity management
A.18 Compliance	
A.18.1 Compliance with legal and contractual requirements	6.3 Plan the SMS
A.18.2 Information security reviews	8.7.3.2 Information security controls

Annex C
(informative)

Comparison of terms and definitions between ISO/IEC 27000:2018 and ISO/IEC 20000-1:2018

Table C.1 provides a comparison of terms defined in ISO/IEC 27000, which is the glossary for terms used in ISO/IEC 27001, and terms defined or used in ISO/IEC 20000-1.

Those with grey highlight have significant correlations. Areas with no shading are those where there is little or no overlap in definitions.

NOTE The harmonized structure for management system standards is described in Annex SL of the ISO/IEC Directives, Part 1. Some of the notes to entry for ISO/IEC 20000-1 refer to Annex SL and not the harmonized structure. These notes have been quoted exactly as they are published in ISO/IEC 20000-1.

Table C.1 — Comparison of terms and definitions between ISO/IEC 27000 and ISO/IEC 20000-1

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
access control	3.1 means to ensure that access to assets is authorized and restricted based on business and security requirements	Not defined or used	No direct equivalent The term "access control" is not used in ISO/IEC 20000-1 but "access" is used in the definition of "service request", in ISO/IEC 20000-1:2018, 7.5.3.2, harmonized structure wording, and for access to information such as configuration information, service catalogue and service continuity plans.
asset	Not defined	3.2.1 item, thing or entity that has potential or actual value to an organization Note 1 to entry: Value can be tangible or intangible, financial or non-financial, and includes consideration of risk and liabilities. It can be positive or negative at different stages of the asset life. Note 2 to entry: Physical assets usually refer to equipment, inventory and properties owned by the organization. Physical assets are the opposite of intangible assets, which are non-physical assets such as leases, brands, digital assets, use rights, licences, intellectual property rights, reputation or agreements. Note 3 to entry: A grouping of assets referred to as an asset system could also be considered as an asset. Note 4 to entry: An asset can also be a configuration item. Some configuration items are not assets. [SOURCE: ISO/IEC 19770-5:2015, 3.2, modified — Note 4 to entry contains new content.]	See 6.2.2 for an explanation of the use of the term "asset" in ISO/IEC 27001 and ISO/IEC 20000-1.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
attack	3.2 attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset	Not defined or used	No direct equivalent
audit (harmonized structure term)	3.3 systematic, independent and documented process 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: An internal audit is conducted by the organization itself, or by an external party on its behalf. Note 3 to entry: "Audit evidence" and "audit criteria" are defined in ISO 19011.	3.1.1 Identical definition and notes to entry	Identical harmonized structure definitions
audit scope	3.4 extent and boundaries of an audit [SOURCE: ISO 19011:2011, 3.14, modified — Note 1 to entry has been deleted.]	Not defined or used	No direct equivalent
authentication	3.5 provision of assurance that a claimed characteristic of an entity is correct	Not defined or used	No direct equivalent

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
authenticity	3.6 property that an entity is what it claims to be	Not defined	The term "authenticity" is used in ISO/IEC 20000-1:2018, 3.2.6, Note 1 to entry, for the term "information security" in the normal English language usage.
availability	3.7 property of being accessible and usable on demand by an authorized entity	3.2.16 service availability ability of a service or service component to perform its required function at an agreed instant or over an agreed period of time Note 1 to entry: Service availability can be expressed as a ratio or percentage of the time that the service or service component is actually available for use compared to the agreed time.	The term "service availability" is used in ISO/IEC 20000-1 when it is necessary to distinguish this specifically defined term from the normal English use of the term "availability". The term "availability" is used in ISO/IEC 20000-1:2018, 3.2.6, for the definition of "information security" and ISO/IEC 20000-1:2018, 3.2.19, for the definition of "service".
base measure	3.8 measure defined in terms of an attribute and the method for quantifying it Note 1 to entry: A base measure is functionally independent of other measures. [SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modified — Note 2 to entry has been deleted.]	Not defined or used	No direct equivalent
competence (harmonized structure term)	3.9 ability to apply knowledge and skills to achieve intended results	3.1.2 Identical definition	Identical harmonized structure definitions
confidentiality	3.10 property that information is not made available or disclosed to unauthorized individuals, entities, or processes	Not defined	The term "confidentiality" is used in ISO/IEC 20000-1:2018, 7.5.3.1, in the normal English language usage. ISO/IEC 20000-1:2018, 7.5.3.1, is a harmonized structure requirement.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
configuration item (CI)	Not defined	3.2.2 element that needs to be controlled in order to deliver a service or services	Configuration management is prominent in ISO/IEC 20000-1. An information asset in ISO/IEC 27001 can also be a CI in ISO/IEC 20000-1. See 6.2.2 for a further explanation about configuration items.
conformity (harmonized structure term)	3.11 fulfilment of a requirement	3.1.3 Identical definition. ISO/IEC 20000-1 has added a note to entry: Note 1 to entry: Conformity relates to requirements in this document as well as the organization's SMS requirements. Note 2 to entry: The original Annex SL definition has been modified by adding Note 1 to entry.	Broadly the same meaning in ISO/IEC 27001 and ISO/IEC 20000-1.
consequence	3.12 outcome of an event affecting objectives Note 1 to entry: An event can lead to a range of consequences. Note 2 to entry: A consequence can be certain or uncertain and, in the context of information security, is usually negative. Note 3 to entry: Consequences can be expressed qualitatively or quantitatively. Note 4 to entry: Initial consequences can escalate through knock-on effects. [SOURCE: ISO Guide 73:2009, 3.6.1.3, modified — Note 2 to entry has been changed after "and".]	Not defined	The term "consequence" is used in ISO/IEC 20000-1:2018, 3.1.20, notes to entry for the term "risk", ISO/IEC 20000-1:2018, 6.1.3, NOTE 1, ISO/IEC 20000-1:2018, 8.1, requirements and ISO/IEC 20000-1:2018, 10.1.1, requirements. The word is used in the normal English language usage. All except ISO/IEC 20000-1:2018, 6.1.3, are harmonized structure text.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
continual improvement (harmonized structure term)	3.13 recurring activity to enhance performance	3.1.4 identical definition	Identical harmonized structure definitions
control	3.14 measure that is modifying risk Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk. Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect. [SOURCE: ISO Guide 73:2009, 3.8.1.1, modified — Note 2 to entry has been changed.]	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 20000-1:2018, 8.7.3, "Information security management". The other use is in ISO/IEC 20000-1:2018, 7.5.3, which is taken almost verbatim from ISO 9001:2015. "Control" is used as a verb in many places in ISO/IEC 20000-1, usually as: "control of XXX process" or "X shall be controlled by Y".
control objective	3.15 statement describing what is to be achieved as a result of implementing controls	Not defined or used	No direct equivalent
correction	3.16 action to eliminate a detected nonconformity	Not defined	The term "correction" is used in ISO/IEC 20000-1:2018, 10.2, NOTE, in the normal English language usage.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
corrective action (harmonized structure term)	3.17 action to eliminate the cause of a nonconformity and to prevent recurrence	3.1.5 action to eliminate the cause or reduce the likelihood of recurrence of a detected nonconformity or other undesirable situation Note 1 to entry: The original Annex SL definition has been changed by adding text to the original "action to eliminate the cause of a nonconformity and to prevent recurrence".	ISO/IEC 27000 has used the harmonized structure definition unchanged. ISO/IEC 20000-1 has added Note 1 to entry to explain that it has adapted the definition to fit service management where it is not always possible or desirable to eliminate the cause of a nonconformity. It is important to distinguish between a nonconformity and underlying root cause(s) of a problem, which are not the same. See "preventive action".
customer	Not defined	3.2.3 organization or part of an organization that receives a service or services EXAMPLE Consumer, client, beneficiary, sponsor, purchaser. Note 1 to entry: A customer can be internal or external to the organization delivering the service or services. Note 2 to entry: A customer can also be a user. A customer can also act as a supplier.	In ISO/IEC 20000-1, the customer can additionally act as a supplier and is also an interested party. In ISO/IEC 27001, a customer is an interested party.
derived measure	3.18 measure that is defined as a function of two or more values of base measures [SOURCE: ISO/IEC/IEEE 15939:2017, 3.8, modified — Note 1 to entry has been deleted.]	Not defined or used	No direct equivalent

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
documented information (harmonized structure term)	3.19 information required to be controlled and maintained by an organization and the medium on which it is contained Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer to — the management system, including related processes; — information created in order for the organization to operate (documentation); — evidence of results achieved (records).	3.1.6 Identical definition and Notes 1 and 2 to entry. Example added: EXAMPLE Policies, plans, process descriptions, procedures, service level agreements or contracts. Note 3 to entry added: Note 3 to entry: The original Annex SL definition has been modified by adding examples.	Identical harmonized structure definitions
effectiveness (harmonized structure term)	3.20 extent to which planned activities are realized and planned results achieved	3.1.7 Identical definition	Identical harmonized structure definitions
event	3.21 occurrence or change of a particular set of circumstances Note 1 to entry: An event can be one or more occurrences and can have several causes. Note 2 to entry: An event can consist of something not happening. Note 3 to entry: An event can sometimes be referred to as an “incident” or “accident”. [SOURCE: ISO Guide 73:2009, 3.5.1.3, modified — Note 4 to entry has been deleted.]	Not defined	This word “event” is used in ISO/IEC 20000-1, in its normal English sense: something that occurs or happens. For example, it is used in the definition of an incident – see ISO/IEC 20000-1:2018, 3.2.5, in this table. This usage is similar to that in ISO/IEC 27001, so is broadly comparable. See “information security event” in this table.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
external context	3.22 external environment in which the organization seeks to achieve its objectives Note 1 to entry: External context can include the following: — the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; — key drivers and trends having impact on the objectives of the organization; — relationships with, and perceptions and values of, external stakeholders. [SOURCE: ISO Guide 73:2009, 3.3.1.1]	Not defined or used	The term "external context" is not used in ISO/IEC 27001 or ISO/IEC 20000-1. However, it is relevant in ISO/IEC 27001:2013, 4.1, and ISO/IEC 20000-1:2018, 4.1, "Understanding the organization and its context". This requires determination of external and internal issues.
external supplier	Not defined	3.2.4 another party that is external to the organization that enters into a contract to contribute to the planning, design, transition, delivery or improvement of a service, service component or process Note 1 to entry: External suppliers include designated lead suppliers but not their sub-contracted suppliers. Note 2 to entry: If the organization in the scope of the SMS is part of a larger organization, the other party is external to the larger organization.	ISO/IEC 20000-1 includes references to, and requirements for, the management of: a) external suppliers b) internal suppliers c) customers acting as suppliers. All contribute to the overall service and are controlled and managed by the organization in ISO/IEC 20000-1:2018, 8.2.3, and ISO/IEC 20000-1:2018, 8.3.4. ISO/IEC 27001 uses the term "supplier" primarily in control A.15.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
governance of information security	3.23 system by which an organization's information security activities are directed and controlled	Not defined or used	No direct equivalent
governing body	3.24 person or group of people who are accountable for the performance and conformity of the organization Note 1 to entry: The governing body can, in some jurisdictions, be a board of directors.	Not defined or used in ISO/IEC 20000-1. However, it is defined in ISO/IEC 20000-10:2018, 3.3.1, and used in the guidance parts of the ISO/IEC 20000 series.	The definition of "governing body" in ISO/IEC 20000-10 is: "group or body that has the ultimate responsibility and authority for an organization's activities, governance and policies and to which top management reports and by which top management is held accountable Note 1 to entry: Not all organizations, particularly small organizations, will have a governing body separate from top management. Note 2 to entry: A governing body can include, but is not limited to, board of directors, committees of the board, supervisory board, trustees, or overseers. [SOURCE: ISO 37001:2016]".

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
incident	See “information security incident”	3.2.5 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 or user	There is a difference between the use of “incident” in ISO/IEC 27001 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: — ISO/IEC 20000-1:2018, 3.2.10, “problem” (see definition in this annex); — ISO/IEC 20000-1:2018, 3.2.9, “known error” (see definition in this annex); — “major incident”, which is not defined in ISO/IEC 20000-1:2018, is considered as the highest category of impact.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
			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 management process, with a requirement that there is a special procedure for managing major incidents. See 6.2.6 for further explanation about incident management.
indicator	3.25 measure that provides an estimate or evaluation	Not defined or used	No direct equivalent
information need	3.26 insight necessary to manage objectives, goals, risks and problems [SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]	Not defined or used	No direct equivalent
information processing facilities	3.27 any information processing system, service or infrastructure, or the physical location housing it	Not defined or used	No direct equivalent

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
information security	3.28 preservation of confidentiality, integrity and availability of information Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.	3.2.6 Identical definition and note to entry	The definitions are identical to ensure alignment between ISO/IEC 27001 and ISO/IEC 20000-1.
information security continuity	3.29 processes and procedures for ensuring continued information security operations	Not defined or used	ISO/IEC 27000 focuses on 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" in this table.
information security event	3.30 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 can be security relevant	Not defined	"Information security event" is only used as part of the definition in ISO/IEC 20000-1:2018, 3.2.7, "information security incident".
information security incident	3.31 single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security	3.2.7 Identical definition	The definitions are identical to ensure alignment between ISO/IEC 27001 and ISO/IEC 20000-1. ISO/IEC 20000-1:2018, 8.7.3, includes requirements about "information security incidents". Incident management requirements are in ISO/IEC 20000-1:2018, 8.6.1. See 6.2.6 for further explanation about incident management.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
information security incident management	3.32 processes for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents	Not defined or used	See definitions in this table for: “incident” “information security incident” “known error” “problem”
information security management system (ISMS) professional	3.33 person who establishes, implements, maintains and continuously improves one or more information security management system processes	Not defined or used	No direct equivalent
information sharing community	3.34 group of organizations that agree to share information Note 1 to entry: An organization can be an individual.	Not defined or used	No direct equivalent
information system	3.35 set of applications, services, information technology assets, or other information-handling components	Not defined or used	No direct equivalent
integrity	3.36 property of accuracy and completeness	Not defined.	The word “integrity” is used in ISO/IEC 20000-1 in its normal English sense: the quality or state of being whole and unimpaired. It is used in ISO/IEC 20000-1:2018, 3.2.6, for the definition of information security, in ISO/IEC 20000-1:2018, 7.5.3.1, harmonized structure text, in ISO/IEC 20000-1:2018, 8.2.6, and ISO/IEC 20000-1:2018, 8.5.3.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
interested party (preferred term) stakeholder (admitted term) (harmonized structure term)	3.37 person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity	3.1.8 person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity related to the SMS or the services Note 1 to entry: An interested party can be internal or external to the organization. Note 2 to entry: Interested parties can include parts of the organization outside the scope of the SMS, customers, users, community, external suppliers, regulators, public sector bodies, non-government organizations, investors or employees. Note 3 to entry: Where interested parties are specified in the requirements of this document, the interested parties can differ depending on the context of the requirement. Note 4 to entry: The original Annex SL definition has been modified by deleting the admitted term "stakeholder", adding "related to the SMS or the services" to the definition and by adding Notes 1, 2 and 3 to entry.	ISO/IEC 20000-1 has edited the harmonized structure definition and added notes to entry. The intent is the same across ISO/IEC 27001 and ISO/IEC 20000-1.
internal context	3.38 internal environment in which the organization seeks to achieve its objectives Note 1 to entry: Internal context can include:	Not defined or used	The term "internal context" is not used in ISO/IEC 27001 or ISO/IEC 20000-1. However, it is relevant in ISO/IEC 27001:2013, 4.1, and ISO/IEC 20000-1:2018, 4.1, "Understanding the organization and its context". This requires determination of external and internal issues.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
	— governance, organizational structure, roles and accountabilities; — policies, objectives, and the strategies that are in place to achieve them; — the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); — information systems, information flows and decision-making processes (both formal and informal); — relationships with, and perceptions and values of, internal stakeholders; — the organization's culture; — standards, guidelines and models adopted by the organization; — form and extent of contractual relationships. [SOURCE: ISO Guide 73:2009, 3.3.1.2]		

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
internal supplier	Not defined	3.2.8 part of a larger organization that is outside the scope of the SMS that enters into a documented agreement to contribute to the planning, design, transition, delivery or improvement of a service, service component or process EXAMPLE Procurement, infrastructure, finance, human resources, facilities. Note 1 to entry: The internal supplier and the organization in the scope of the SMS are both part of the same larger organization.	No direct equivalent
known error	Not defined	3.2.9 problem that has an identified root cause or a method of reducing or eliminating its impact on a service	No direct equivalent but see "incident" and "problem".
level of risk	3.39 magnitude of a risk expressed in terms of the combination of consequences and their likelihood [SOURCE: ISO Guide 73:2009, 3.6.1.8, modified — "or combination of risks" has been deleted in the definition.]	Not defined or used	No direct equivalent
likelihood	3.40 chance of something happening [SOURCE: ISO Guide 73:2009, 3.6.1.1, modified — Notes 1 and 2 to entry have been deleted.]	Not defined	Although not defined, the term "likelihood" is used in ISO/IEC 20000-1:2018 in the definition of "corrective action", Notes 2 and 4 to entry to the definition of "risk" and in ISO/IEC 20000-1:2018, 6.1.3, NOTE 1.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
management system (harmonized structure term)	3.41 set of interrelated or interacting elements of an organization to establish policies and objectives and processes to achieve those objectives. Note 1 to entry: A management system can address a single discipline or several disciplines. Note 2 to entry: The system elements include the organization's structure, roles and responsibilities, planning and operation. Note 3 to entry: The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.	3.1.9 Identical definition. Notes 1 and 3 to entry are identical. ISO/IEC 20000-1 has edited Note 2 to entry to: The management system elements include the organization's structure, roles and responsibilities, planning, operation, policies, objectives, plans, processes and procedures. Note 4 to entry added: Note 4 to entry: The original Annex SL definition has been modified by clarifying that the system is a management system and listing further elements in Note 2 to entry.	Identical harmonized structure definitions Note 2 to entry has slight variation between ISO/IEC 27001 and ISO/IEC 20000-1.
measure	3.42 variable to which a value is assigned as the result of measurement [SOURCE: ISO/IEC/IEEE 15939:2017, 3.15, modified — Note 2 to entry has been deleted.]	Not defined	Although not defined, the term "measure" is used in ISO/IEC 20000-1:2018, 8.5.2.2, to design new or changed measures as needed for the SMS.
measurement (harmonized structure term)	3.43 process to determine a value	3.1.10 Identical definition	Identical harmonized structure definitions
measurement function	3.44 algorithm or calculation performed to combine two or more base measures [SOURCE: ISO/IEC/IEEE 15939:2017, 3.20]	Not defined or used	No direct equivalent

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
measurement method	3.45 logical sequence of operations, described generically, used in quantifying an attribute with respect to a specified scale Note 1 to entry: The type of measurement method depends on the nature of the operations used to quantify an attribute. Two types can be distinguished: — subjective: quantification involving human judgment; and — objective: quantification based on numerical rules. [SOURCE: ISO/IEC/IEEE 15939:2017, 3.21, modified — Note 2 to entry has been deleted.]	Not defined	ISO/IEC 27001:2013, 9.1, and ISO/IEC 20000-1:2018, 9.1, have a requirement to determine "the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results".
monitoring (harmonized structure term)	3.46 determining the status of a system, a process or an activity Note 1 to entry: To determine the status, there may be a need to check, supervise or critically observe.	3.1.11 Identical definition and note to entry	Identical harmonized structure definitions
nonconformity (harmonized structure term)	3.47 non-fulfilment of a requirement	3.1.12 Identical definition ISO/IEC 20000-1 has added a note to entry: Note 1 to entry: Nonconformity relates to requirements in this document as well as the organization's SMS requirements.	Identical harmonized structure definitions

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
non-repudiation	3.48 ability to prove the occurrence of a claimed event or action and its originating entities	Not defined	Non-repudiation is used in ISO/IEC 20000-1:2018, 3.2.6, Note 1 to entry, for the term "information security" in the normal English language usage.
objective (harmonized structure term)	3.49 result to be achieved Note 1 to entry: An objective can be strategic, tactical, or operational. Note 2 to entry: Objectives can relate to different disciplines (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 to entry: An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as an information security objective or by the use of other words with similar meaning (e.g. aim, goal, or target). Note 4 to entry: In the context of information security management systems, information security objectives are set by the organization, consistent with the information security policy, to achieve specific results.	3.1.13 Identical harmonized structure definition and Note 1 to entry. Note 2 to entry has been modified to: Note 2 to entry: Objectives can relate to different disciplines [such as financial, health and safety, service management and environmental goals] and can apply at different levels [such as strategic, organization wide, service, project, product and process]. Notes 3 and 4 to entry refer to an SMS and the service management objectives and policy. Note 5 to entry added: Note 5 to entry: The original Annex SL definition has been modified by adding "service management" and "service" to Note 2 to entry.	Broadly the same meaning in ISO/IEC 27001 and ISO/IEC 20000-1.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
organization (harmonized structure term)	3.50 person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives 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.	3.1.14 Identical definition and Note 1 to entry. Notes 2, 3 and 4 to entry have been added: Note 2 to entry: An organization or part of an organization that manages and delivers a service or services to internal or external customers can be known as a service. Note 3 to entry: If the scope of the SMS covers only part of an organization, then organization, when used in this document, refers to the part of the organization that is within the scope of the SMS. Any use of the term organization with a different intent is distinguished clearly. Note 4 to entry: The original Annex SL definition has been modified by adding Notes 2 and 3 to entry.	Identical harmonized structure definitions. In both ISO/IEC 27001 and ISO/IEC 20000-1, the organization may be part of a larger entity, such as a company or charity. See “service provider” which can be used by organizations providing services.
outsource	3.51 make an arrangement where an external organization performs part of an organization’s function or process Note 1 to entry: An external organization is outside the scope of the management system, although the outsourced function or process is within the scope.	3.1.15 Identical definition and note to entry	Identical definitions

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
performance (harmonized structure term)	3.52 measurable result Note 1 to entry: Performance can relate either to quantitative or qualitative findings. Note 2 to entry: Performance can relate to the management of activities, processes, products (including services), systems or organizations.	3.1.16 Identical definition and Note 1 to entry. Note 2 to entry has been modified to: Note 2 to entry: Performance can relate to the management of activities, processes, products, services, systems or organizations. Note 3 to entry added: Note 3 to entry: The original Annex SL definition has been modified by adding "services" to Note 2 to entry.	Identical harmonized structure definitions
policy (harmonized structure term)	3.53 intentions and direction of an organization as formally expressed by its top management	3.1.17 Identical definition	Identical harmonized structure definitions
problem	Not defined	3.2.10 cause of one or more actual or potential incidents	See "incident" and "known error" in this table. See 6.2.7 for further explanation about problem management.
procedure	Not defined	3.2.11 specified way to carry out an activity or a process Note 1 to entry: Procedures can be documented or not. [SOURCE: ISO 9000:2015, 3.4.5]	The definition used by ISO/IEC 20000-1 is based on that in ISO 9000. They are broadly similar. Only the note to entry differs, i.e. in ISO 9000, procedures can be undocumented, but ISO/IEC 20000-1 references to procedures are all to "documented procedure". Those procedures in ISO/IEC 20000-1 that are part of a plan are documented as part of the plan.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
process (harmonized structure term)	3.54 set of interrelated or interacting activities which transforms inputs into outputs	3.1.18 set of interrelated or interacting activities that use inputs to deliver an intended result Note 1 to entry: Whether the "intended result" of a process is called output, product or service depends on the context of the reference. Note 2 to entry: Inputs to a process are generally the outputs of other processes and outputs of a process are generally the inputs to other processes. Note 3 to entry: Two or more interrelated and interacting processes in series can also be referred to as a process. Note 4 to entry: Processes in an organization are generally planned and carried out under controlled conditions to add value. Note 5 to entry added: Note 5 to entry: The original Annex SL definition has been changed from "set of interrelated or interacting activities which transforms inputs into outputs". The original harmonized structure definition has also been modified by adding Notes 1 to 4 to entry. The revised definition and Notes 1 to 4 to entry are sourced from ISO 9000:2015, 3.4.1.	The harmonized structure definition used in ISO/IEC 27000 has been modified in ISO/IEC 20000-1 to use the definition from ISO 9000 and its notes to entry. This is to reflect the process usage where not all inputs are transformed into outputs but deliver results. The difference in definitions is not significant.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
record	Not defined or used in the main text of ISO/IEC 27001.	3.2.12 document stating results achieved or providing evidence of activities performed EXAMPLE Audit reports, incident details, list of training delegates, minutes of meetings. Note 1 to entry: Records can be used, for example, to formalize traceability and to provide evidence of verification, preventive action and corrective action. Note 2 to entry: Generally, records need not be under revision control. [SOURCE: ISO 9000:2015, 3.8.10, modified — EXAMPLE has been added.]	The ISO/IEC 20000-1 definition is based on ISO 9000:2015 including notes to entry with the addition of examples specific to ISO/IEC 20000-1. ISO/IEC 27001 uses the phrase "documented information" instead of the term "record", except in A.18.1.3, "Protection of records".
release	Not defined or used	3.2.13 collection of one or more new or changed services or service components deployed into the live environment as a result of one or more changes	No direct equivalent See 6.3.6 for further explanation about release and deployment management.
request for change	Not defined or used	3.2.14 proposal for a change to be made to a service, service component or the SMS Note 1 to entry: A change to a service includes the provision of a new service, transfer of a service or the removal of a service that is no longer required.	ISO/IEC 27001:2013, Annex A, refers to "change management" as a control in A.10.1.2. Many controls in ISO/IEC 27001:2013 refer to the management or control of changes. For example: A.8.3, A.10.1, A.10.2.3 and A.12.5.1.

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
reliability	3.55 property of consistent intended behaviour and results	Not defined	The term "reliability" is referred to in ISO/IEC 20000-1:2018, 3.2.6, "information security": Note 1 to entry: In addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved.
requirement (harmonized structure term)	3.56 need or expectation that is stated, generally implied or obligatory Note 1 to entry: "Generally implied" means that it is custom or common practice for the organization and interested parties that the need or expectation under consideration is implied. Note 2 to entry: A specified requirement is one that is stated, for example, in documented information.	3.1.19 Identical harmonized structure definition and Notes 1 and 2 to entry. ISO/IEC 20000-1 has added Note 3 to entry: Note 3 to entry: In the context of an SMS, service requirements are documented and agreed rather than generally implied. There can also be other requirements such as legal and regulatory requirements. Note 4 to entry added: Note 4 to entry: The original Annex SL definition has been modified by adding Note 3 to entry.	Identical harmonized structure definitions
residual risk	3.57 risk remaining after risk treatment Note 1 to entry: Residual risk can contain unidentified risk. Note 2 to entry: Residual risk can also be referred to as "retained risk".	Not defined or used	No direct equivalent

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
review	3.58 activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives [SOURCE: ISO Guide 73:2009, 3.8.2.2, modified — Note 1 to entry has been deleted.]	Not defined	Although not defined, there are many requirements in ISO/IEC 20000-1 to review various items.
review object	3.59 specific item being reviewed	Not defined or used	No direct equivalent
review objective	3.60 statement describing what is to be achieved as a result of a review	Not defined or used	No direct equivalent

Table C.1 *(continued)*

Term	ISO/IEC 27000:2018	ISO/IEC 20000-1:2018	Comments on usage of the term in both standards
risk (harmonized structure term)	3.61 effect of uncertainty on objectives 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 its consequence or likelihood. Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and consequences (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these. Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated" likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) 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 will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.	3.1.20 effect of uncertainty Notes 1 to 4 to entry are identical	ISO/IEC 27000 includes Notes 5 and 6 to entry with 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 organizational objectives. ISO/IEC 20000-1 has adopted the exact harmonized structure definition. ISO/IEC 27001 has adopted the definition from ISO 31000, which is the same as that in the harmonized structure but has the addition of "on objectives". See "vulnerability" and "threat" in this table. See 6.2.5 for further explanation about risk and other parties.