FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27013**

ISO/IEC JTC **1**/SC **27**

Secretariat: DIN

Voting begins on:
2021-08-26

Voting terminates on:
2021-10-21

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

Reference number
ISO/IEC FDIS 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 life cycle 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*

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 life cycle, 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 and ISO/IEC 20000-1 for 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 standard which can be merged and how they can be merged;

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, 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 configuration items 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 life cycle. 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.