

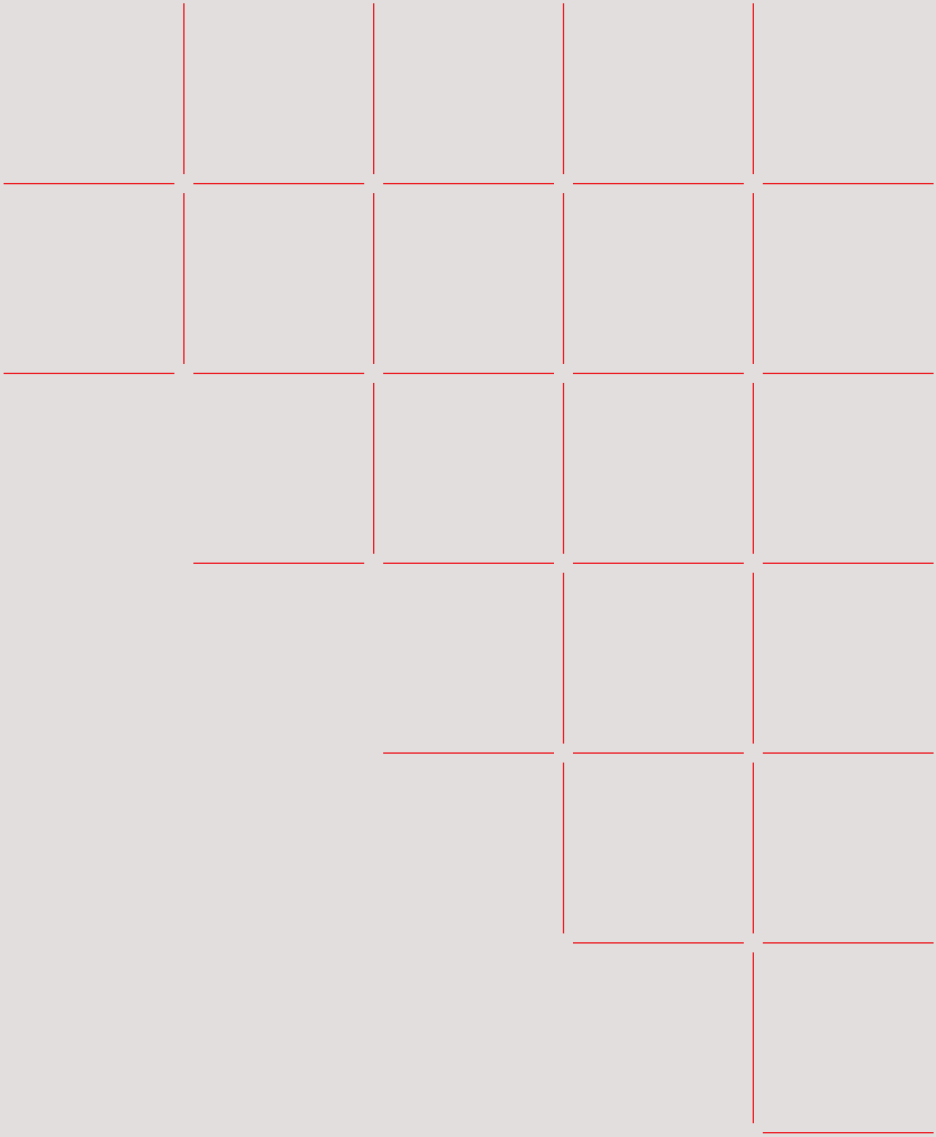
ISO/IEC 27001:2022

Information Security Management Systems

A practical guide for SMEs

Advice from ISO/IEC JTC 1/SC 27

iec.ch
iso.org



Foreword

Cybercrime is on the rise, growing increasingly severe and sophisticated as hackers develop ever more advanced techniques. In this fast-changing landscape, it can seem difficult or even impossible to keep track of cyber-risks. At ISO, we are ready with support and solutions to help small and medium-sized enterprises (SMEs) safely navigate this process.

This handbook focuses on guiding SMEs in developing and implementing an information security management system (ISMS) in accordance with ISO/IEC 27001, in order to help protect yourselves from cyber-risks.

SMEs account for the vast majority of businesses worldwide and often have specific needs. International Standards help you to compete on a level playing field with bigger enterprises, gaining access to global markets, reducing costs and building customer confidence that your products are safe and reliable. We understand the unique challenges you face as SMEs – whether due to lack of money, resources or a full understanding of the issues – that can lead to your security being compromised.

ISO/IEC 27001 is the world's leading standard for ISMSs, providing organizations with guidance on establishing, implementing, maintaining and continually improving an ISMS. It defines requirements for an ISMS and helps organizations secure their information assets by identifying and managing risks – something which is vital in today's digital world. The requirements that ISO/IEC 27001 describes are generic and are designed to be both scalable and flexible, and hence apply to all types of organization, regardless of their size or the nature of their business activities or sector.

Implementing ISO/IEC 27001 means that your organization or business has put in place a system to manage risks related to the security of data owned or handled by the company, and that this system respects all the best practices and principles enshrined in the standard.

By using ISO/IEC 27001, you demonstrate to stakeholders and customers that you are committed to managing information securely and safely. It is a unique way to promote your organization, celebrate your achievements and prove that you can be trusted. In addition, the holistic approach of ISO/IEC 27001 means that the entire organization is covered, not just IT. People, technology and processes all benefit.

This handbook was developed by experts from the joint ISO and IEC technical community on information security, cybersecurity and privacy protection. I sincerely hope it will support your enterprise's efforts in developing an ISMS that acts as a tool for risk management, cyber-resilience and operational excellence. By doing so, we hope your organization will set the standard and emerge as a leader in your industry.



Sergio Mujica
ISO Secretary-General

Contents

Foreword	3
About this handbook	6
Information security management systems	8
Using the handbook	10
Guidance on what ISO/IEC 27001 means to SMEs	13
Terminology	14
The Foreword of ISO/IEC 27001	16
Introduction	17
1. Scope	18
2. Normative references	19
3. Terms and definitions	19
4. Context of the organization	20
5. Leadership	28
6. Planning	36
7. Support	63
8. Operations	75
9. Performance evaluation	79
10. Improvement	85
Annex A – Frequently asked questions	90
Annex B – Certification	95
Annex C – Websites and International Standards	104

About this handbook

The aim of this handbook is to guide small and medium-sized enterprises (SMEs) on developing and implementing an information security management system (ISMS), based on the International Standard ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection — *Information security management systems — Requirement*.

The remainder of this handbook will refer to this standard as ISO/IEC 27001 for brevity. The requirements that ISO/IEC 27001 describes are generic and are designed to be both scalable and flexible, and hence apply to all types of organization, regardless of their size or the nature of their business activities or the sector. This handbook focuses on guiding SMEs.

Strictly speaking, an SME is in practice an *organization*. However, SMEs do not normally consider themselves as organizations, as the term typically refers to an entity which is larger in size and complexity. Therefore, this handbook frequently uses the term enterprise, which is consistent with the recognized concept of SMEs.

In this context, the term enterprise includes all organizations that use, process, exchange and store information for their own internal needs and on behalf of others, such as their customers or suppliers. Examples of enterprises are small family businesses, manufacturers, distributors, schools, retail outlets, law firms, charitable foundations, care homes and community medical centres,

This handbook consists of a number of sections that readers can apply and refer to separately, as the need arises. As such, the handbook is a supporting document for SMEs applying ISO/IEC 27001. Therefore, this handbook neither adds requirements, nor modifies existing ones.

When compared with larger entities, SMEs face particular challenges when developing an ISMS, such as the availability of resources. With a limited number of employees, an SME might not be able to dedicate a team to manage an ISMS. Therefore, individuals within an SME would be expected to include information security in addition to their main roles. Another challenge is the cost involved in developing and maintaining an ISMS. There are many factors that mean the costs can be lower than those in a large organization. Communications, for example, can often be simple and more direct, decision-making is usually simpler, involving just a few people, management can be more straightforward due to simpler structures, and risk management is generally less complicated.

From an SME's perspective, the time and money spent on an ISMS should be seen as an investment, providing business opportunities while showing a return on the investment, including protecting the enterprise's information and providing assurance and confidence to its customers. As ISO/IEC 27001 is a flexible and scalable standard, these challenges should not be a barrier to a small enterprise implementing the standard.

Information security management systems

What is an ISMS?

A management system is defined as a set of interrelated or interacting elements of an organization to establish policies and objectives, as well as processes to achieve those objectives. In simple terms, a management system is the way an enterprise directs and controls those business activities that are related (either directly or indirectly) to achieving its intended objectives and results.

For an ISMS, the objectives are the preservation of the confidentiality, integrity and availability of the information under its control. Your business activities should be directed, controlled and managed in a way that achieves these information security objectives. This needs to consider the requirements of relevant interested parties in the planning, operation and management of your ISMS in order to achieve these objectives. For example, an interested party could be one of your customers and their requirements associated with your products and services.

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS.

ISO/IEC 27001 should not be confused with other security standards; for example those which specify explicit requirements and techniques for protecting IT products, networks and services. ISO/IEC 27001 specifies requirements for good management practices in order to achieve information security management but without referencing any particular type of IT product, network or service.

Implementing and using an ISMS should not result in excessive rules, paperwork and documentation, or lack of flexibility, and it should not be a financial burden. The implementation, use and maintenance of an ISMS should be considered an investment that will provide a return in the form of benefits and improvements to your information security.

All enterprises will already have some form of management system in place and this should be the basis on which their information management system is built. Therefore, it is likely that your enterprise could already fulfil at least some of the requirements included in ISO/IEC 27001 but has simply not yet organized its activities into a formal ISMS.

Why have an ISMS?

It is a strategic decision of the enterprise whether to implement an ISMS. It does so to protect its information against threats and risks. Such threats can include, for example the online theft or unauthorized modification of information. Customers might also want assurances that an enterprise protects their information. Moreover, there could be a law or regulation that requires certain types of information be protected, such as personal data.

An ISMS provides a systematic approach to fulfilling the information security objectives and requirements of an enterprise, which should lead to improvements to information security.

Using the handbook

Target audience

The target audience for this handbook is SMEs. This includes all types of small enterprise, covering all kinds of business activity and different styles of management and ownership that differentiates them from medium and large organizations.

Getting started

Initially, SMEs should use this handbook to understand both the requirements of ISO/IEC 27001, and what an ISMS is.

It is important to note that it is not the intention of ISO/IEC 27001 to impose a totally new way of managing an enterprise. An enterprise should continue to use its existing management processes as much as possible and adapt or extend them, if necessary, to implement an effective ISMS. For an enterprise to follow this advice, it should look at how it manages its business and how it currently operates in order to customise its systems where necessary, to satisfy the requirements of ISO/IEC 27001. Hence an enterprise does not need to start from the very beginning; it should use what is already in place and adapt this as necessary.

A small enterprise will have many management aspects related to its business that are more straightforward and less complex than those of a medium-to-large organization. For example, decision-making is often a less complicated process. Therefore, for a small enterprise these examples can be advantageous and make the implementation of ISO/IEC 27001 much easier.

Therefore, you will need to analyse which requirements of ISO/IEC 27001 apply to your enterprise and whether or not you are satisfying these requirements.

If you are using the 2013 version of ISO/IEC 27001, you will need to review your current practices, and then update them to satisfy the requirements of the 2022 version.

Getting help and support

There are many sources that give information and advice (see Annex C):

- industry or professional associations, especially those that can provide guidance to SMEs;
- government departments that specialise in SME support and advice;
- national standards bodies;
- Internet websites containing information about ISMS, for example, ISO (iso.org/standard/27001, committee.iso.org/home/jtc1sc27);
- training course providers;
- certification bodies;
- consultants.

These sources may help you understand what your enterprise needs to do to implement an ISMS. Next, your enterprise needs to decide whether to go ahead with an ISMS. If your enterprise decides to go ahead, it then needs to determine how much of the work it can do and how much help it needs from external sources.

Your enterprise will need to consider what resources (people and time) it has available to do the work and this will determine how much additional help it might need. Again, the sources listed above may be able to provide additional help but your enterprise will need to take account of any associated costs.

Before using external sources of help, the following need to be noted and considered:

- Your ISMS will be unique to your enterprise; therefore, any generic solutions provided by external sources cannot always be adapted to your specific needs and business requirements.
- Two areas of misunderstanding and common failure are:
    - Not all levels of management get involved – ISO/IEC 27001 requires all levels of management to commit to the ISMS and get involved in its operation.
    - Your personnel do not get actively involved when implementing the ISMS – ISO/IEC 27001 requires commitment and participation at all levels of an enterprise. For example, consultants may not replace your management or personnel, nor may consultants manage your enterprise, speak, lead or make decisions on your behalf.

Implementing the ISMS yourself

Taking into account these requirements and the available resources, your enterprise may either implement an ISMS with or without external support – this is a decision that only an enterprise's management can make.

It is important to remember that it is your enterprise that has overall responsibility for its own ISMS. This responsibility cannot be delegated or assigned outside your enterprise even if you use an external source, such as a consultant.

There is no reason for you to make significant changes to the way your enterprise operates or manages its business. Some aspects of your enterprise may need to be adapted to meet the requirements of ISO/IEC 27001, but it is up to your enterprise how you are going to implement the standard – ISO/IEC 27001 is flexible and able to be used by all organizations and enterprises. There is no requirement in ISO/IEC 27001 for significant changes to be made to your current way of doing business.

Using a consultant

If you decide to use a consultant to help and guide you through implementing the requirements in ISO/IEC 27001, then you need to be rigorous in your selection. Also, you need to be clear what a consultant can do for you and what they should not do. A consultant could help you with a preliminary assessment of your current activities compared with the requirements of ISO/IEC 27001, and training and awareness and some aspects of implementation. However, a consultant cannot be responsible or accountable for implementing the ISMS, make management decisions, or take the leadership or ownership roles for your ISMS.

When selecting a consultant, your enterprise should undertake a thorough and careful examination of the qualifications, credentials, references and knowledge and experience of ISMS.

There needs to be a clear understanding between your enterprise and the consultant regarding scope of work, roles and responsibilities, milestones, confidentiality agreements, impartiality, regular and effective communications and reporting and any specific requirements of the enterprise. In order to inspire ownership of the ISMS and commitment to it, people in your enterprise should be actively working with the consultant.

Information security management system certification

Certification is a demonstration that your ISMS conforms to the requirements of ISO/IEC 27001 and is carried out by an independent third party. Certification of an ISMS is not mandatory; it is the decision of your enterprise. There are several factors that might influence your decision; for example, one of the customers to whom you supply products or services could request certification, there may be statutory or regulatory requirements for certification or it might give you a competitive advantage if you gain certification. Annex B of this handbook provides more details about certification.

Guidance on what ISO/IEC 27001 means to SMEs

According to the World Bank[1], SMEs account for the vast majority of businesses worldwide and are important contributors to global economic development and job creation. SMEs represent about 90% of businesses globally – and approximately 99% in the European Union – while SMEs provide more than half of all employment. Therefore, it can be said that, collectively, SMEs form the largest set of businesses in the world.

The specialist, international working groups that write International Standards have created such standards to assist SMEs, just as they do for larger organizations. In particular, SMEs should be able to share in the gains and benefits in efficiency and effectiveness offered by ISO/IEC 27001.

This handbook briefly summarises the requirements of each clause and subclause of ISO/IEC 27001, and then provides guidance to help understand these requirements. The guidance also includes examples and case studies.

1 https://www.worldbank.org/en/topic/smefinance

Terminology

When using ISO/IEC 27001, note that certain words and phrases have particular significance or meaning specific to their context. The following verbal forms have a specific meaning in ISO and are applicable to all ISO documents.

Verbal form	Definition
shall	to express requirements – alternative words are: is to, must, needs to
should	to express recommendations
may	to express permission
can	to express possibility or capability

For most words used in ISO/IEC 27001 the dictionary definition applies, particularly common terms.

Some terms specific to information security management systems are shown below, while ISO 27000 describes the vocabulary applied to ISMS:

Term	Definition
audit	systematic and independent process for obtaining evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled
availability	property of being accessible and usable on demand by an authorized entity
competence	ability to apply knowledge and skills to achieve intended results

Term	Definition
confidentiality	property that information is not made available or disclosed to unauthorized individuals, entities, or processes
continual improvement	recurring activity to enhance performance
corrective action	action to eliminate the cause of a nonconformity and to prevent recurrence
effectiveness	extent to which planned activities are realized and planned results achieved
integrity	property of accuracy and completeness
nonconformity	non-fulfilment of a requirement
objective	result to be achieved
objective evidence	data supporting the existence or verity of something
performance	measurable result
requirement	need or expectation that is stated, generally implied or obligatory
review	activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives
risk	effect of uncertainty on objectives
top management	person or group of people that directs and controls an organization at the highest level

How to use this handbook

This handbook follows the same structure of ISO/IEC 27001, and reflects the ten sections (or clauses of this International Standard. Each section and subsection will begin with a short summary of the requirements of each specific clause or subclause of ISO/IEC 27001, and then provides guidance on what this means and what an enterprise needs to do. Additionally, there are also case studies which provide examples of how organizations can meet the requirements of ISO/IEC 27001.

Lastly, this handbook does not duplicate the clauses in ISO/IEC 27001, so a reader should refer to the applicable clauses of the standard when reading the handbook.

The Foreword of ISO/IEC 27001

The Foreword of ISO/IEC 27001 lists the technical details of ISO's processes of standards writing and approval. It also explains that ISO/IEC 27001:2022 cancels and replaces the 2013 edition, which has been technically revised to align with the Harmonized Structure for management system standards. Annex A of ISO/IEC 27001 has also been extensively revised and to align with the information security controls described in ISO/IEC 27002:2022.

Introduction

Introduction, 0.1 – General

The Introduction describes the purpose of ISO/IEC 27001, which is to establish, implement, maintain and improve an ISMS. It then describes the factors that influence the form, scale and function of an ISMS, and the outcomes of implementing an effective ISMS.

This section adds that ISO/IEC 27001 is a foundation standard for ISMS, and exists in a family of International Standards in the ISO/IEC 27000 series.

How you run your enterprise is unique to you. ISO/IEC 27001 gives you a framework to create suitable management practices that applies to your organization. The standard specifies requirements for an ISMS that have been recognized as being aligned with internationally accepted good practice for running an organization.

The standard specifies a set of items that need to be included in an ISMS, but it does not specify how you do them. Hence, there is considerable freedom and flexibility in meeting the information security requirements of the standard.

You need to build your ISMS around your existing enterprise practices and processes, i.e. the practices you currently use, so that it becomes part of and integrated within your current overall management structure and processes.

This subclause indicates that you do not need to align your documentation with the clause structure of the standard, nor use the specific terminology in it; instead, you can use the terms that you normally use in your organization.

An ISMS aims to give confidence that your enterprise is preserving the confidentiality, integrity and availability of information by applying a risk management process. This in turn provides assurance to interested parties that an enterprise is managing risks adequately, and that it is meeting any associated statutory and regulatory requirements.

Introduction, 0.2 – Compatibility with other management system standards

This part of the Introduction to ISO/IEC 27001 describes how the standard uses the Harmonized Structure that is now applied within all management system standards. This structure is specified in the ISO Directives, Part 1, and sets out a format of ten sections containing mandatory text for all management system standards.

Therefore, the Harmonized Structure provides a standard, harmonized framework for all management systems. This in turn helps those enterprises which want to implement a single management system based on the requirements of two or more management system standards.

Following the Introduction, ISO/IEC 27001 specifies ten clauses which conform to the ISO High Level Structure. The first three clauses, which are the *Scope, Normative references and Terms and definitions*, do not contain mandatory requirements. The remaining seven clauses do contain normative or mandatory elements, and are therefore assessable for both internal and external audits.

1. Scope

This describes the extent of application of ISO/IEC 27001, for ISMS that apply to all types and sizes of organization whose activities require the management and control of information security.

Guidance

The Scope explains the purpose of the standard. This clause states that the requirements of ISO/IEC 27001 are for an ISMS and focuses attention on the preservation of the confidentiality, integrity and availability of information by applying a risk management process to give confidence to interested parties that risks are adequately managed and that the ISMS meets customer requirements and applicable statutory and regulatory requirements.

It also indicates that ISO/IEC 27001 is intended to be generic and applicable to all organizations, regardless of their type or size or the products and services they provide.

2. Normative references

This clause states which International Standards are mandatory and in this case, there is only one such reference, which is ISO/IEC 27000, Information technology — Security techniques — *Information security management systems — Overview and vocabulary*.

Guidance

If a reference is normative, this means that users of ISO/IEC 27001 must refer to the normative reference and apply it. ISO/IEC 27000 describes an overview of ISMS and also describes the vocabulary for this field of application. Therefore, your enterprise must know and understand the contents and language of ISO/IEC 27000, and use the same language when referring to information security and ISMS.

ISO/IEC 27000 is a standard that contains a number of information security definitions, including those terms used in ISO/IEC 27001.

Considering that ISO/IEC 27000 is a mandatory reference, it is advisable that your enterprise at least has access to both these International Standards.

Other references are listed in Annex C of this handbook (References).

3. Terms and definitions

The activities described in every International Standard have their own terminology. ISO/IEC 27001 does not list any specific terminology, but instead refers to ISO/IEC 27000, which includes the vocabulary applied to ISMS.

Guidance

In many ISO standards, this clause contains a list of terms and their definitions necessary for an understanding of the text; however, as all terminology required for the use of ISO/IEC 27001 is given in ISO/IEC 27000, you are directed to that standard instead.

The International Standards that ISO/IEC JTC 1/SC 27 has developed for both information security management and ISMS use generic terms to describe the relationship between the interested parties involved.

ISO hosts a useful online browsing platform (OBP) which includes a large compendium of terms and definitions here: https://www.iso.org/obp.