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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Contents

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

4. Context of the organization

This clause in ISO/IEC 27001 consists of four subclauses, which are:

4.1 Understanding the organization and its context

4.2 Understanding the needs and expectations of interested parties

4.3 Determining the scope of the ISMS

4.4 ISMS

Each of these is explored in turn.

Subclause 4.1 – Understanding the organization and its context

The organization must determine the internal and external issues that are relevant to its business purpose and that have an effect on its powers to achieve the intended results of its ISMS.

The standard recommends that users refer to ISO 31000:2018, *Risk management Guidelines*, subclause 5.4.1 of ISO 31000.

Guidance

The intent of this subclause is to understand the enterprise and its context by determining the external and internal issues that are relevant to the business purpose and strategic direction of your enterprise, and how this might have an effect on its ability to achieve the intended results of its ISMS (i.e.. the preservation of the confidentiality, integrity and availability of information).

External and internal issues can and do change - this can have an effect on the ability of the ISMS to preserve the confidentiality, integrity and availability of information. Therefore, you should make sure that the ISMS and its context within the enterprise is monitored and reviewed at planned intervals and through activities such as management review.

Information about external and internal issues can be gathered from many sources, such as through internal documents, discussions and meetings (detailing information about the enterprise, its mission and procedure). External sources of information might include national and international press, relevant websites and government departments, small business and

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

professional associations, professional and technical publications, workshops and conferences and meetings with customers and other interested parties. The information gathered from external sources needs to be understood and adapted in the context of your enterprise; you need only consider that which is important and relevant to your enterprise and not become overwhelmed by the volume of information from external sources, such as the media and websites. It is more important to take note of information from customers, clients and suppliers that you do business with.

Examples of external issues can include, but are not limited to:

- **economic factors**, that may have an impact on the enterprise and its ISMS, such as national economy, money exchange rates, interest rates, inflation, credit availability, wages, transportation costs;
- **social factors**, such as unemployment rates, safety requirements, education levels, public, culture;
- **political conditions**, such as political stability, public investments, local infrastructure, international trade agreements;
- **technological trends** that may have an impact on the enterprise and its ISMS; this could be new technology and its adoption by the enterprise, new versions of software, materials and equipment or patent expirations:
- **contractual relationships**, understanding your relationships with customers and suppliers and considering their requirements for information security where appropriate to the provision of services and products;
- **market factors**, including market share, market trends, customer growth trends, domestic and global issues, market stability, supply chain relationships;
- **statutory and regulatory factors** which affect the business, such as privacy regulations, cybersecurity laws, employment law, competition regulations, import/export restrictions, intellectual property law, trade union regulations and regulations related to a specific industry.

Internal issues can include:

- the overall **performance** of the enterprise;
- **resource factors**, including infrastructure, environment for the operation

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

of the ISMS;

- **human aspects**, including competence of persons, the culture of the enterprise, relationships with unions;
- **operational factors**, such as process/production and service provision capabilities, performance of the ISMS, monitoring customer satisfaction;
- **governance of the organization**, such as rules and procedures for decision-making or organizational structure.

The approach your enterprise takes to establish the context and determine the issues is entirely yours to decide. A simple approach can be useful for your enterprise (dependent on the size and complexity of its business), such as brainstorming meetings and asking 'what if?' questions. Your enterprise may decide to use a SWOT analysis tool (strengths, weaknesses, opportunities and threats).

Case study

A small enterprise importing goods for distribution for the car servicing trade is a part of a supply chain. It handles various type of information, including that from foreign suppliers, exporters, border control systems and customers. The enterprise should determine any external issues that may affect the ability of the ISMS to protect this information.

Case study

A small enterprise provides transport services to schools and is implementing an ISMS to protect all information related to the provision of these services and its customers. The local government has various requirements related to the security and safety of the children that the enterprise needs to comply with.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

Case study

A small residential care-home for elderly people providing accommodation, 24-hour professional care, special medical needs and other support services. The care home handles a lot of sensitive and personal information, including medical data, financial data and personal data relating to its patients. The care home is implementing an ISMS to protect all information related its patients, staff and carers. The enterprise might need to comply with several government regulations and the ISMS would need to include provisions for these regulations.

Subclause 4.2 – Understanding the needs and expectations of interested parties

The organization has to determine which interested parties are relevant to the ISMS, together with their requirements, and which of these requirements need to be addressed within the ISMS.

Guidance

The intent of this subclause is to make sure that your enterprise considers the relevant requirements of all relevant interested parties. This covers more than just those of your immediate customers and helps to focus attention on those parties that have an interest in your enterprise, which could have an impact of your ISMS. Subclause 4.1 of ISO/IEC 27001 helps to determine the relevant interested parties.

Each enterprise may generally have a different set of interested parties, so your enterprise will have a relatively distinct set of interested parties. An interested party may be identified by their possible influence or impact on the performance of your enterprise and the decisions it needs to make. Of course, your enterprise may be affected by the decisions that an interested party makes.

An interested party may create risks to your ISMS, for example, a member of a supply chain connected to your system whose security is not good. Another consideration in determining an interested party could be their potential influence or impact on the market.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Examples of interested internal parties include:

- owners;
- shareholders;
- employees;
- staff.

Examples of interested external parties include:

- customers, clients;
- business partners;
- external providers and suppliers;
- users;
- others working for the enterprise;
- bankers and insurance providers;
- statutory and regulatory authorities;
- owners of intellectual property;
- unions;
- trade associations;
- competitors.

Understanding the needs and expectations of interested parties can be achieved in different ways. For example, consulting with customers and suppliers, conducting user surveys, reviewing supply chain relationships, reviewing regulatory requirements and consideration of feedback received for interested parties, market surveillance and monitoring customer needs.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

A small international language school has students from around the world learning English and French. The age of the students is 11 years and upwards. The courses that the school offers are provided through classroom teaching and online teaching. It handles various types of information related to its students (including any special needs, expectations), admissions and the administration of the school. The school needs to ensure it understands the needs and expectations of its students, parents and guardians and the requirements of educational authorities, regulatory bodies and border control agencies (e.g. student visas) in order to protect the information it handles in an appropriate and suitable way.

Subclause 4.3 – Determining the scope of the information security management system

This subclause requires the organization to determine its ISMS scope by considering the context, interested parties and the connections and dependencies of the activities the organization performs, and those of other organizations.

Guidance

The intent of this subclause is for your enterprise to determine the boundaries of your ISMS. These boundaries must be defined in a way that helps your organization satisfy the requirements of ISO/IEC 27001 and the objectives of your ISMS.

This means for that ISO/IEC 27001, 4.3, a) and b), your enterprise should establish the scope based on the external and internal issues as determined by the requirements of ISO/IEC 27001 4.1 and the relevant requirements of relevant interested parties as determined in accordance with the requirements in ISO/IEC 27001, 4.2.

For ISO/IEC 27001, 4.3, c), the enterprise should also establish the boundaries of the ISMS by considering the infrastructure of the organization, whether it has more than one site, its activities, any commercial policies it has and whether its activities, processes and services are provided internally or externally.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

The scope should be recorded and maintained as documented information. The scope should include details of all that is covered by an ISMS. This documented information can be maintained in whatever method your enterprise determines meets its needs, such as manual or electronic.

Case study

A small independent book seller imports and sells books in many countries. When considering the scope of the ISMS of the book seller, relevant factors can include the following: there are two sites for its operations, i.e. an office and storage facility; it works with publishers (at home and overseas), second-hand booksellers, antique-book auctioneers, and other book suppliers, logistics companies and customers.

Subclause 4.4 – ISMS

This subclause states that the organization has to establish, implement, maintain and continually improve an ISMS, applying the requirements of ISO/IEC 27001.

Guidance

The intent of this subclause is to ensure that you establish, implement, maintain and continually improve an ISMS in accordance with ISO/IEC 27001. This includes the processes needed for the effective implementation of the system, such as risk assessment, risk treatment, monitoring, internal audit, management review and others, in accordance with the requirements of ISO/IEC 27001.

A process is a series of actions or steps taken in order to achieve a particular end. Each process will use a set of inputs in order to produce an intended result. The level to which processes need to be detailed can vary according to the context of the enterprise and the application of risk – taking into consideration the extent to which the process affects the ability of your enterprise to achieve its intended results, the likelihood of problems occurring with the process and the potential consequences of such problems.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

A process is a set of interrelated or interacting activities that use inputs and outputs to deliver intended results. For example, the inputs needed for the planning of the ISMS (ISO/IEC 27001, subclause 6.1) include aspects referenced in ISO/IEC 27001, subclause 4.1, and the requirements referred to in ISO/IEC 27001, subclause 4.2. This will determine the risks and opportunities that need to be addressed. Specifically, to:

- ensure the ISMS can achieve its objectives;
- prevent or reduce undesired effects;
- achieve continual improvement.

The output of this process includes actions needed to address the risks and opportunities. The processes required for risk assessments are covered in detail under Clause 6.

Case study

A cheese manufacturer wants to meet the requirements of ISO/IEC 27001. It already has information security, including keeping some of its business information in the form of papers, files and folders, which are kept physically safe and secure, and its buildings, shop and office are physically secure. It has started to use IT to store and process more of its information electronically and has started to promote and sell some of its cheeses online. It is also expanding to open more shops.

The manufacturer has internal meetings to look at everything in its business to determine the issues (ISO/IEC 27001, subclause 4.1) and requirements (ISO/IEC 27001, subclause 4.2) to understand its business and future plans involved in its cheese-making activities or to record that tasks were performed as required. This includes reviewing the information it has, both paper-based and electronic: what information is vital and necessary for its future business, information that is not vital but should be retained and information that can be discarded.

The review includes identifying what information is either sensitive or confidential for the enterprise, and what information that is publicly available (e.g. information on their Website promoting their products) and also includes requirements for protecting the information.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

5. Leadership

Clause 5 of ISO/IEC 27001 includes three subclauses with requirements for leadership, which are:

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

Subclause 5.1 – Leadership and commitment

This subclause specifies eight actions top management need to take in order to provide leadership in order to ensure the overall effectiveness of the ISMS.

Guidance

The intent of this subclause is to demonstrate the management leadership and commitment to the ISMS. It does this by requiring management to be directly involved in certain activities.

The enterprise's management should know what they want their enterprise to achieve. The same should be true for information security, and there should be a clear vision of what achievements are desired from having an ISMS. It is an investment because good information security will cost money and time, but the reward should be a safer, more successful business. ISO/IEC 27001 refers to what the enterprise's management wants to achieve as *objectives*, and the policy is the overarching statement of intent describing what the enterprise will do to achieve these objectives. The requirement is that top management of the enterprise must ensure that the information security policy for the enterprise reflects their intention and direction.

Examples

An objective could be "no inappropriate disclosure of personal information"; a corresponding policy could be "laptops must use hard disc encryption".

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Information security should never be an afterthought. This is what is meant by “integration”. It should be a natural part of everyday operations. The enterprise’s management should therefore encourage themselves (and everyone who works under their direction) to “think security first” in all their work.

Examples

Risk assessment should form a natural first step in any new undertaking. Reviewing the results of any activity and seeking improvements should likewise be second nature.

Running an effective ISMS requires time and effort. The enterprise’s management must therefore ensure that there are adequate resources, including budget for technology and people, and that people have the necessary competence to perform their work. If this is not done, planned activities will not happen on time and the ISMS will never meet its objectives. Of course, if the enterprise is a one-person entity, then this person is responsible for all the requirements in ISO/IEC 27001, 5.1 d), f) and h).

Case study

A photographer runs a one-person photographic enterprise and is responsible for everything from marketing, sales to taking the photographs and making the tax returns. The photographer has invested in a high-end digital camera and mobile computing equipment and makes use of cloud services for storage, processing and customer communications. Customers include newspapers and television companies.

The photographer operates a mobile ISMS to assist with information security management, which is considered integral to business operations. The photographer employed a consultant to help build the ISMS and ensure that it was fully integrated into the workflow and did not distract the photographer from concentrating on the business of taking newsworthy photographs and making a profit.

The enterprise’s management should be fully aware of how the ISMS is performing and act as necessary to ensure that it meets its objectives.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

A small medical practice consists of five doctors, four nurses, a practice manager and three receptionists. The most senior doctor acts as management for the ISMS and, being concerned about the confidentiality, integrity and availability of medical data, has taken personal responsibility for the ISMS. Weekly meetings are held before the practice is opened for patients, at which the senior doctor ensures that all matters relevant to information security are discussed.

In enterprises that consist of more than one person, it is important for the enterprise's management to set an example of how management requires other people to behave. It is also important for everyone to know why the enterprise has an ISMS and what can happen if the enterprise does not conform. The enterprise's staff should understand why things should be performed in a certain way, as well as how things should be performed. By knowing why, people can use their initiative when something that they are supposed to do cannot be done, but an alternative exists which achieves the same result.

Case study

An electronics company has a government contract. The last person out must store all documents marked "confidential" in Safe Number 1. The purpose of this procedure is to safeguard government secrets. However, one evening the staff member discovers that this cannot happen because the lock is broken.

Understanding the purpose of the procedure, the employee looks for another safe with a working lock and sufficient space to accommodate the entire contents of Safe Number 1. Safe Number 3 is suitable.

The employee transfers the contents of Safe Number 1 to Safe Number 3, together with the "confidential" documents to be put away and locks it. Finally, the employee pins a note on Safe Number 1, explaining what they have done and why. They know the importance of this last step. The following morning their colleagues will find Safe Number 1 open and empty. Without the note, they might falsely conclude that there has been a burglary and raise an alarm.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

The enterprise's management should also encourage and support everyone engaged in ISMS activities. Subordinate management should be encouraged to emulate the behaviour of the enterprise's management. In this way, the benefits of leading by example cascade down throughout the enterprise.

Case study

Having been taught how to perform a risk assessment, a senior police officer decided to buy a safe and lock up all their confidential documents overnight. News of what the senior officer had done quickly spread throughout the department. Within a week, all the subordinate officers had bought safes for themselves and their staff, so that they could secure their documents overnight too.

Such encouragement and support not only demonstrate the enterprise's management commitment to information security but also provides vital feedback to everyone that they are doing what is required of them. It facilitates reward, when justified. The enterprise's management should also encourage people to report mistakes, errors and incidents, as early detection can avoid disasters, create awareness and lead to ISMS improvements.

Case study

Office entry is controlled by key card. Upon leaving a social gathering after work, an employee discovered that they had lost their key card. They immediately phoned their line manager and reported what had happened. The line manager was able to deregister the card immediately. It therefore could not be used by anyone to gain access to the office. The next day, the employee was reminded to be more careful, but nevertheless congratulated for their prompt action in reporting the incident. No harm had been done.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

The enterprise's management should always be looking for improvements: more rewarding objectives, more efficient operations, greater personal and customer satisfaction. Ideas for improvement can come from anywhere and anyone.

Example

An enterprise's management realizes that world events can have an impact on their business operations. The management therefore adds an item to the regular management meetings to take note of recent world events and determine their impact, if any, on the enterprise and its information security concerns. While there are many world events that do not have any impact on the enterprise, there is no longer a risk of missing those that do.

Subclause 5.2 – Policy

This subclause requires the organization to establish a policy and specifies the details that must be included within the ISMS policy.

Guidance

The intent of this subclause is to require the enterprise's management to record what they wish their enterprise to achieve and how they want that to be approached. The policy must be a true reflection of what the enterprise's management wants the ISMS to achieve and how they want it to be done. It should be appropriate for their business purposes.

Case study

The director of a one-person IT consultancy business has an ISMS. Its policy has sections for cloud service providers; operation of the enterprise's software as a service; the enterprise's public Website; information back-up; password reminders; critical updates and malware; end-point and wireless security; retention of records; disposal of media; information in transit; working away from the office; and security breaches.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

The enterprise's management can either include the enterprise's information security objectives in the policy or write down the way they are to be determined.

Case study

The owner of a five-person motorcycle workshop reviews the performance of the workshop near the end of each budget year and sets new business objectives for the coming year. The owner then sets new information security objectives in support of these business objectives, taking account of incidents, and feedback from the workshop staff and customers. The workshop's information security policy describes the way in which the enterprise's management sets the information security objectives for the enterprise.

While the enterprise's management can best demonstrate commitment through action, a simple policy statement along the lines of "[Name of the enterprise] is committed…" is recommended. Likewise, the enterprise's management can best demonstrate their commitment to continual improvement through action. Nevertheless, a simple policy statement like "[Name of the enterprise] is committed…" is recommended.

The information policy must be documented and the enterprise may decide exactly how to do this, e.g. digitally, as a hard copy, or both forms.

Example

It can be a document called "Information security policy". It can be part of a document called the "Operations manual", it could be a Webpage or even posted on a wall.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

In enterprises that consist of more than one person, since the enterprise's management wants everyone to obey the information security policy, they must first be informed.

It is also possible that people outside of the enterprise might need to be aware of the policy, either because they need to see it before they will trade with the enterprise or because the enterprise wants them to comply with it. Whichever the case, the enterprise should be able to decide which parts it is willing to make available, how and to whom.

Case study

A small taxi company has contracts with the local council for driving physically and mentally challenged children to various special needs schools. The drivers are appropriately vetted and are trained in how to take care of their passengers in the event of an accident or medical emergency. The council therefore has an interest in the details of the taxi company's ISMS policy, which the company makes available in its entirety to the council.

Subclause 5.3 – Organizational roles, responsibilities and authorities

This subclause requires top management to assign and communicate all responsibilities and authorities for roles relevant to the ISMS. There are also requirements for ensuring responsibility and authority such that the ISMS conforms to the requirements of ISO/IEC 27001, and for reporting to top management the performance of the ISMS.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Guidance

The intent of this subclause is to require the enterprise's management to assign responsibility for the ISMS.

The enterprise management can determine and assign whichever responsibilities and authorities that they consider necessary for the smooth operation of the ISMS. However, ISO/IEC 27001 does ask for two special roles to be assigned. If the enterprise's management takes day-to-day responsibility for the ISMS, then the enterprise's management should assign these two special roles to themselves. If not, it would be appropriate to assign them to the person that they put in charge of the ISMS.

Case study

In a sixty-person logistics business, the managing director owns the ISMS and chairs the management review meetings. However, the quality manager has the responsibility for ensuring conformity to the quality and information security manual and for reporting formally to the board of directors on quality and information security performance.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

6. Planning

Clause 6 of ISO/IEC 27001 specifies the requirements for planning and consists of three subclauses, which are:

6.1 Actions to address risks and opportunities

6.2 Information security objectives and planning to achieve them

6.3 Planning of changes

The first subclause is divided into three subsections, with the first subsection describing the general requirements, while the second and third subsections specify the requirements for risk assessment and treatment respectively.

Subclause 6.1 – Actions to address risks and opportunities

6.1.1 General

The organization has to examine the context of the organization under subclauses 4.1 and 4.2, and then ascertain the risks and opportunities that the organization needs to address. This is to minimize or eliminate the chances of risks compromising the effective operation of the ISMS, and also to capitalize on any opportunities that would benefit the ISMS.

Guidance

This subclause requires an enterprise to determine and address the risks and opportunities associated with the needs and expectations of interested parties. These parties include customers, clients, users and regulators. Risk has many definitions; however, for the purposes of this handbook, risk can be understood as situations that can expose the enterprise to harmful consequences that could result in a negative impact. Such impacts in turn could seriously affect the enterprise's finances, reputation, operations, customers, clients or users.

Risk can be expressed in terms of sources causing the risk, the effect or consequences of this cause and the likelihood of this occurring. The cause could be an incident such as an unauthorized attempt to access information,

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

resulting in its theft. In simple terms, risk is typically expressed as the potential for an incident (such as unauthorized access to your information) to exploit the vulnerabilities (weaknesses) in your access control system resulting in the theft of information.

It is important to note that business activities provide benefits and opportunities and these should be considered along with information security risks. Enterprises use information to carry out their business and to achieve their business goals and objectives. For example, to increase business, deliver faster and better services, or to present a competitive advantage in the market. However, controlling risks to this information is important. Therefore, an enterprise needs to achieve a balance between controlling risks to information security, but not do so to the extent that reduces opportunities.

Your enterprise needs to address the issues and requirements relevant to its business determined in ISO/IEC 27001, subclauses 4.1 and 4.2 and subsequently determine the risks and opportunities in order to ensure the ISMS can achieve its intended outcome(s), to prevent or reduce undesired effects and to achieve continual improvement.

Case study

A newly established community health-clinic provides medical services to 29 000 patients. Some of its computers are connected through the Internet to pharmacies, other local health centres, a local hospital and the central government health service. One of the main requirements this clinic has is the protection of the medical records of its patients. Most of these medical records are stored electronically, but some older records from other health clinics are in paper form. Another requirement is protecting the access to its computers and Internet connections. The clinic will need to determine the risks it faces by undergoing a risk assessment.

Your enterprise needs to adopt a plan that will specify actions to address the risks and opportunities. The plan will also need to specify how it intends to integrate and implement the actions into its ISMS processes and how it will evaluate the effectiveness of these actions.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

6.1.2 Information security risk assessment

This subclause requires an enterprise to have a systematic process for determining the information security risks to its business, and then assess these risks by considering both the chances of an incident happening, and the severity of the consequences. The enterprise needs to document this process in a procedure.

Guidance

The intent of this subclause is to define an information security risk-assessment process. Your enterprise needs to decide on what methods and criteria it uses to identify, analyse and evaluate risks, including the criteria for accepting the level of risk. Whatever method is adopted it must enable risk assessments and re-assessments to produce results in a repeatable, valid, consistent and comparable way. ISO/IEC 27001 provides a lot of flexibility for your enterprise to select the method most suited for its business. The method used should give you an understanding of the risks the enterprise faces, typically in terms of risk causes and effects (consequences and impacts) and the likelihood of risk occurrence, the levels of risk and criteria to decide if the level of risk is acceptable.

a) Define and document risk-acceptance criteria

ISO/IEC 27001 uses the term *criteria* to refer to a principle or standard by which something may be judged or decided. The risk-acceptance criteria are defined by your enterprise and refer to the level of risk the enterprise is willing to accept. These criteria will depend on the risk appetite of the enterprise, i.e. the level of risk the enterprise is willing to pursue and tolerate. It also depends on the risks to the business objectives, which need to take account of internal and external interests and requirements, any relevant standards that might apply to the enterprise and applicable laws and regulations.

The risk-acceptance criteria can be based on the likelihood of the risk occurring and consequence or impact, but it can be extended to consider other factors such as the cost-benefit balance between prospective losses and the cost of controls.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

b) Develop criteria for performing information security risk assessments

The criteria to perform a risk assessment will specify how the significance of a risk is determined in terms of its consequences, likelihood and level of risk.

In ISO/IEC 27001 we are concerned with the consequences that directly or indirectly have an impact on the preservation or loss of confidentiality, integrity and availability of information. Therefore, consequence criteria should be developed and defined in terms of the level of damage or loss, or harm to the enterprise resulting from the loss of confidentiality, integrity and availability of information.

When defining consequence criteria, the following should be particularly considered:

- loss of life or harm to individuals or groups;
- loss of staff and intellectual capital;
- financial losses;
- operational losses, productivity losses, system failures, damages to a business process;
- loss of business advantage or market share;
- damage to public trust or reputation;
- breaches of legal, regulatory or statutory requirements;
- breaches of contracts or service levels.

An enterprise with an appetite for risk can set a higher threshold of acceptance, meaning it accepts more risks than an organization with a lower-risk appetite.

The risk criteria should be reviewed and updated as necessary as a result of any changes in the context of information security risk management.

The risk-acceptance criteria should be approved by the authorized management level.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Example

The risks associated with a data breach will depend on the type of data. If it is sensitive data, then it can have an impact on personal data and can lead to non-compliance with applicable legislation for protecting personal data, e.g. while if it is critical data – such as financial data, such as access codes and account numbers, then it can have a severe impact on a business process and operations. Alternatively, the impact of a data breach might be a breach of contract, damage to customer trust or the loss of a business advantage.

The likelihood of the risk occurring will depend on different criteria. For example, if it is a:

- natural event;
- accidental event or human error;
- technology failure;
- degree of exposure to a threat;
- degree of vulnerability or weakness.

The likelihood of an incident can be expressed in terms of the chances of something occurring, for example, as a probability, frequency or possibility. The chances of system failure, hardware failure or network failure can be expressed in numerical terms, whereas human error or degree of exposure or weakness is more likely to be expressed qualitatively.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

A small consultancy business helps companies with project management support. It undertakes a risk-assessment exercise for its own business and it uses the following qualitative likelihood scale for their risk analysis:

Impact

- Very high (critical, threatens business survival)
- High (major or significant loss, damage, harm)
- Medium (moderate loss, damage, harm)
- Low (minor loss, damage, harm)
- Very low (very little loss, damage, harm)

Likelihood (description)

- Very high (80% – most certainly will occur)
- High (50%-60% – good chance of occurring)
- Medium (25% – a chance of occurring)
- Low (10% – occurring)
- Very low (less than 1% - very little chance of occurring)

c) Risk identification

This stage of the assessment process involves identification of what could happen that may have an impact on the ISMS of your enterprise. You need to consider the various types of event that could occur that may result in a risk. These are sometimes classified as security incidents, for example a hacking attack, potential breaches, such as a failure to keep your sensitive or commercial information secure in compliance with your information security policy resulting in leakage of this information to the public, or a compromise of security through lack of staff awareness.

Your enterprise will have information in various formats, stored and processed in different ways, for example paper-based information stored in filing cabinets, electronic formats such as databases, hard drives or USB devices, on websites or in the cloud. All these different ways of storing information are subject to security incidents, breaches or compromises that

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

can result in the loss of confidentiality, integrity and availability of information. A common way to identify risks is to consider the potential threats and vulnerabilities that might be related to your information assets. A vulnerability is a weakness that an attacker could exploit, for example, a hacker might exploit the weakness in your access control method to gain unauthorized access to your information.

Case study

A small logistics firm highly reliant on IT and mobile devices to do its business has identified the following threats and incidents relevant to its business:

- **Virus incidents**, meaning its system could be infected by a virus by e-mail, clicking on Website links, using infected CDs and USB memory devices.
- **Inappropriate usage** by staff of the technology used by the enterprise, including use of e-mail and the Internet for non-work purposes.
- **Unauthorized access** involves someone gaining access to your computer systems without your permission or consent. This can be an internal or external threat. In many countries, hacking into a computer is a criminal offence. However, you should not rely on legislation alone to protect you. Although the law might be a deterrent to hackers, you must implement your own additional security controls to prevent unauthorized access. The impact of this threat occurring includes theft of information, deletion of information, modification of information, changing the settings on your computer or gaining access to personal information.
- **Data loss** can involve accidental or deliberate loss. Storage of data, whether in paper form or electronic form, can be vulnerable to data theft or physical damage. It is important to implement back-ups of your data so that your enterprise can continue to do business even though the computer may be damaged and computer data lost.
- **Theft** can take many forms, including theft of money, information, equipment, copyright material, personal details, identity or credit card details.

External theft - Theft of information is a criminal offence and should be reported to the police. These situations are not always straightforward; for example, these types of threat could highlight the vulnerabilities of the enterprise's internal procedures and may result in a loss of reputation. This type of theft should be handled very carefully.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Internal theft – Internal theft needs careful consideration and handling. Internal procedures should cover what to do in such circumstances. Also, human resources should be consulted.

- **System failures, disasters and disruptions** can result from (i) IT hardware and software failures, which may be due to lack of maintenance, component malfunctions, out-of-date software patches, upgrades or physical hazards, (ii) virus infection, leading to destruction of files, software, systems slowing down, overloads or crashes, (iii) a hacking attack, resulting in unauthorized access to system files, deleting or destroying system data or causing a denial of service attack, (iv) sabotage by a member of staff with a grievance or grudge again the enterprise.

A system failure needs careful handling as it may be due to a security breach and this may involve the police. Reporting and recovering from system failures is important in order to get your business back to normal as soon as possible. Such a system failure might only affect part of the enterprise or all of the enterprise. The system failure may be minor and the recovery quick, or major and the recovery takes much longer. The nature and impact of the failures will determine what actions need to be taken to recover.

Also, the enterprise needs to consider if the failure will have an external impact on those enterprises that depend on you, for example, supply chain and customers. Those external parties affected need to be included in the reporting of the incident.

The risk identification process involves gathering information, which can involve interviews with staff, individually or in a team. It might also include feedback and opinions from interested parties such as suppliers, business partners and customers. It is important to note that risk perceptions vary between people. What one person perceives as a risk another person may view differently. Those in control of the identification process need to be aware of the possible variations in opinion from a human perspective and also from a business perspective.

There are many sources of information referencing types of threats, vulnerabilities and risks that your enterprise may wish to consult to establish what risks you face. Some of this information is generic and so will need to be adapted to your particular business situation. Also, it is important not to forget your own records of past incidents that may have happened.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

The output of the risk identification process should be a list of risks, which will then be used during the risk analysis stage (d).

Case study

A small publishing house specialising in technical publications and journals handles a large volume of copyrighted material of high commercial value. It is carrying out a review of its information security and has identified a number of vulnerabilities covering hardware, software, networks, people and infrastructure, including:

- incorrect use of software and hardware;
- insufficient training on security awareness;
- inadequate access control procedures;
- e-mail usage policy not developed;
- procedures for handling copyrighted material insufficient;
- insufficient physical protection of the building and offices;
- lack of or incomplete back-up copies;
- uncontrolled downloading and use of software;
- poor password management;
- unprotected storage;
- lack of hardware maintenance;
- disposal or reuse of storage media without proper erasure.

Your enterprise needs to determine its risk owners. The risk owner is accountable for the risks and they have the management authority for managing the control of risks and for making decisions about the control of the risks. Depending on the size and nature of the enterprise, your enterprise may have one risk owner or several risk owners, each accountable for different types of assets or business function, for example physical, information or operational processes.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Example

A small five-person enterprise might assign one member of staff as risk owner of all information and processes and another member of staff as risk owner of all other risks the enterprise needs to control.

d) Analyse information security risks

This stage of the process deals with determining the level of risk based on the impacts (or consequences) of the risk and the likelihood of the risks occurring. The impact concerns the loss of confidentiality, integrity and availability and its relationship with the business processes and objectives enabled by the use of information and related assets. For example, data theft is a security issue relating to the loss of confidentiality but this also has a wider impact on the business and its objectives.

The severity of this impact may affect some or all of the business; it may represent a minor loss, a major loss or a serious or critical loss. The loss may be financial, fines or penalties or legal costs, loss of operations and productivity, loss of services, loss of sales or orders, or loss of image or reputation, all resulting from a comprise to the information security of the enterprise. This loss might be minimal, having a minor or medium effect on business, through to having some effect on the ability of the business to function and operate normally and, in the worst case, a shut-down of business activities.

As mentioned in a) to c), there are several methods that can be used for the risk-assessment process. ISO/IEC 27001 does not prescribe any particular method and leaves the selection of an appropriate method for the enterprise to decide. Any method can be selected as long as it fulfils the requirement of subclauses 6.1.2 d) 1) to 3) in ISO/IEC 27001.

In assessing the severity of the potential impacts, you can use either a qualitative or quantitative approach. A qualitative approach involves assigning severity levels (e.g. low, medium, high) to each impact. A quantitative approach involves assigning a numerical or measurable value to each impact, for example a financial amount, a productivity value (e.g. a percentage loss) or a service loss in hours of unavailability.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Assessing the likelihood of risk occurrence can be based on historical data of past internal security problems, past incident reports, industry data and statistics, and other sources of data that have recorded the likelihood of the risk occurring.

In determining the level of risk, both the impact value and the likelihood value need to be combined. The following case study example illustrates one way of achieving this.

Case study

A small business uses the following table to calculate the level of risk:

		Likelihood				
		VL	L	M	H	VH
Impact	VH	5	6	7	8	9
	H	4	5	6	7	8
	M	3	4	5	6	7
	L	2	3	4	5	6
	VL	1	2	3	4	5

Risk level map 1

Legend: VL very low, L low, M medium, H high, VH very high

In this table (Risk level map 1), 9 represents a very high level of risk and 1 represents a very low level of risk. As the impact increases from very low to very high and the likelihood also increases in value, then the level of risk increases: the higher the impact and likelihood the higher the risk, whereas the lower the impact and likelihood the lower the risk. If your enterprise uses this method, then it may decide on a different set of scales for its analysis, for example a three-point, four-point, six-point or higher scale. The examples here and elsewhere in this handbook are generic illustrations to describe the overall risk management process.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Another important part of the analysis process is to understand the events, incidents and causes that are likely to have an impact on your information assets. An accidental system failure will cause of loss of availability of information; it may also cause deletion or modification of information.

A deliberate hacking attack on your systems many cause intentional deletion of information, theft of information or the execution of a virus in the system, causing a range of damage. The downloading of a file through an e-mail system may cause damage if the file contains unsafe material. The lack of regular back-ups of information may cause a range of business problems and cause information security problems. These are just a few of the many cause and effect examples that can have a damaging impact on your enterprise.

In assessing the level of risk, it is important to consider what existing information security controls are in place.

Case study

A small design studio providing services to companies wanting a Website for its business is at the stage of risk analysis. It decides to review their existing controls as part of the analysis process to check the relevance and effectiveness of these controls. During the analysis the enterprise discovers the following:

- An existing procedure for use of e-mail attachments which is badly written and needs to be revised. For the experienced user, the procedure is not used as they know how to handle sensitive information; however, to an untrained member of staff there is a risk of sensitive information being sent via e-mail.
- The access control procedure is out-of-date, as it does not cover some of the recent technology that has been introduced in the business.
- The existing processes for disposal or storage of information have resulted in several hardware failures. The enterprise needs to review this situation and then implement a more reliable and effective storage system.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

Your enterprise should adopt the most suitable approach of doing this analysis that is compatible with existing management processes and practices. There are several different ways that might be considered, for example group meetings with management and staff, interviews or discussions with individual members of staff responsible for certain aspects of security, staff questionnaires, reviewing reports of past incidents and security reviews, discussing feedback from customers and business partners. The risk-assessment process is a team effort and engagement and involvement with as many staff members as possible would provide the best results as a greater range of feedback, views and experiences would be available.

e) Evaluate the information security risks

After identifying the risks to information security using the results from the risk analysis (subclause 6.1.2(c) in ISO/IEC 27001), according to the risk criteria (subclause 6.1.2(a) in ISO/IEC 27001), the next step is to determine the scale of these identified risks.

One method of illustrating risk is in terms of likelihood of the threat to your information and the impact of this occurring. These can be represented in a diagram, sometimes referred to as a heat map. The heat maps in Figures 1 and 2 illustrate levels of risk grouped into three colours: dark grey, light grey and white. The dark grey represents a high-risk level, the light-grey medium risk and the white low risk.

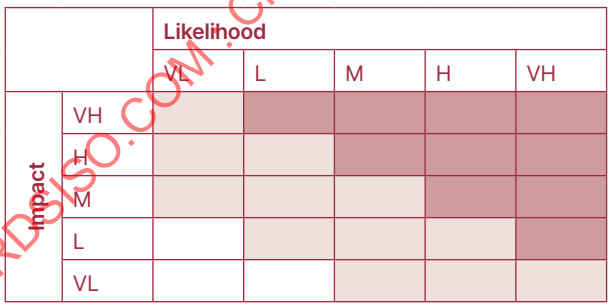

Figure 1 - Risk-heat map 1
Legend: VL very low, L low, M medium, H high, VH very high

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

		Likelihood				
		VL	L	M	H	VH
Impact	VH					
	H					
	M					
	L					
	VL					

Figure 2 - Risk-heat map 2
Legend: VL very low, L low, M medium, H high, VH very high

Risk-heat map 1 in Figure 1 has a lower-risk acceptable level compared to that of risk-heat map 2 in Figure 2, and so one enterprise might choose to use map 1 whereas another might choose map 2.

The risk-heat maps are merely examples to illustrate the theory behind risk evaluation.

Other heat maps may have larger or smaller scales for impacts, for example 4, 6, 7 or 8-point scales or a greater number of different grey areas. See, for example, Figure 3.

		Likelihood						
		VL	L	L-M	M	M-H	H	VH
Impact	VH							
	H							
	M-H							
	M							
	L-M							
	L							
	VL							

Figure 3 - Risk-heat map 2
Legend: VL very low, L low, M medium, H high, VH very high

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Your enterprise defines its own heat map based on its appetite for risk. It is also for your enterprise to decide whether it uses this method; it could choose a different method.

At the risk evaluation stage, your enterprise needs to decide whether the risks are acceptable, or whether you need to reduce the risks to an acceptable level through risk treatment. Using the example of Figure 1, your enterprise decides that the risks in the dark grey are not acceptable; however, in the light-grey area your enterprise might want to do a cost-benefit analysis for any proposed risk treatment and the business opportunities, and then compare this against the business impacts. After this analysis of the light-grey areas, your enterprise might decide to leave some risks in this area and take an action to closely monitor the situation for an early review and reassessment, to check whether the situation does not change and the risk does not move into the dark grey area.

Of course, after this analysis of the light-grey risks, you might decide it is a business benefit to move some risks into the white area through risk treatment. A cost-benefit analysis is a useful technique to determine whether the costs of risk treatment are proportionate, when considering the costs of incidents. Additionally, risk treatment can itself create opportunities, and the cost-benefits of these opportunities should be included in the cost-benefit analysis.

Creating a risk register is good practice. This will be a list of all the risks that you have identified as a result of your risk assessment. It is a good idea to prioritize the list according to the severity of risk from very high to low. Figure 4 shows an example of prioritization in terms of low, medium, high and very high risks.

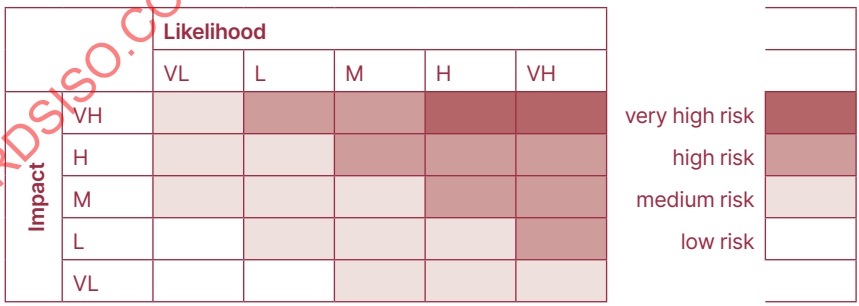

Figure 4 - Risk-heat map 1
Legend: VL very low, L low, M medium, H high, VH very high

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

The prioritization of the treatment of risks helps your enterprise allocate its resources according to this prioritization. For example, risks considered critical might be those associated with severe impacts, which in turn could have a critical effect on the business systems, processes or services of your enterprise. Conversely, incidents with low risks, and with low probabilities of occurrence would most likely not be regarded as critical, high-impact risks, on the other hand, typically require immediate or timely action to either eliminate such risks, or reduce them to acceptable levels.

ISO/IEC 27001, subclause 6.1.2 requires organizations to identify risks, assess them, and document both the process and results of the risk assessment. A risk register is a proven and effective way of doing these tasks. Your enterprise has the freedom to decide how it organizes its risk register. The following is just an example of risk register:

	Description	Assets affected	Comments
Very high risks			
[risk name]			
[risk name]			
High risks			
[risk name]			
[risk name]			
Medium risks			
[risk name]			
[risk name]			
Low risks			
[risk name]			
[risk name]			

Figure 5 – Example risk register

The risk name is a label given to the risk by your enterprise for easy reference. The description could include the threats, incidents, vulnerabilities and impacts associated with the risk. The assets affected could be classified by type of information affected, physical assets, technology, services or processes.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

6.1.3 Information security risk treatment

Firstly, this clause requires the enterprise to select the relevant treatment options for the risks it has determined for information security, and then to determine all those necessary controls for the risk treatment option selected. Finally, your enterprise needs to check the set of determined controls with the set of reference controls in ISO/IEC 27001, Annex A to establish whether any controls have been left out.

Guidance

a) Risk-treatment options

The intent of this subclause is to define the process for treating information risks, such that the risks are either eliminated, or reduced to practical levels so that the residual risks are acceptable. The first step in this process is to determine the appropriate risk-treatment options, which could be used by your enterprise to deal with the results of your risk assessment (ISO/IEC 27001, subclause 6.1.2 and subsection 6.1.2 of this handbook).

The selection of the treatment options should be consistent with the criteria established in subsection 6.1.2 a of this handbook), and the business objectives.

Risk-treatment options include:

- **Knowingly and objectively accept the risk** – it may be that your enterprise may not be able to identify suitable security controls for some risks or the cost of implementing controls outweighs the potential loss of the risk occurring. In these cases, a decision needs to be made whether or not to accept the risk and live with the consequences if the risk occurs. You should document these decisions so that management is aware of its risk position and knowingly accepts the risk.
- **Share or transfer the risk** – transferring or sharing the risk is an option where it might be more difficult to reduce the risk or control it to an acceptable level, or where it might be more economically transferred to a third party. There are several methods for transferring risk to another organization, for example through insurance or via outsourcing. Insurance companies can provide insurance cover once all the relevant underwriting information is supplied (insurance in this case is where an indemnity is provided if the risk falls within the policy cover provided). In using insurance as a risk-sharing mechanism you should identify how much of the actual risk is reduced, and so in practice there will always

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

be some residual risk that you are accountable for. Insurance does not in general provide immediate mitigation in the event of an incident or cyberattack, for example a hacker disrupting your systems.

- **Avoid the risk** – risk avoidance describes any action where your enterprise business activities are changed to avoid the risk occurring. For example:
  - discontinuing certain planned activities such as no longer using the Internet for certain business activities;
  - moving assets from an area of risk, such as no longer storing sensitive files in a certain location as they are not sufficiently protected;
  - deciding not to process sensitive information, such as with a third party, if sufficient protection cannot be guaranteed.

Risk avoidance should be balanced against the business and financial needs of your enterprise. For example, it might be essential to use the Internet because of business demands, despite concerns about hackers, or it might not be feasible to move certain information assets and their storage facilities to a safer place. In such cases, one of the other options, risk transfer or risk reduction, should be considered.

- **Reduce the risk** – this involves implementing a set of security controls according to the results of your risk assessment. A set of controls should be selected for all those risks you have decided should be reduced to the level identified as acceptable or at least to a level in accordance with the acceptance criteria of your enterprise. In identifying and selecting controls it is important to consider the security requirements related to the risks, for example the threats and vulnerabilities, legal and regulatory requirements, contractual obligations and all other findings from the risk assessment.

There is no universal or standardized approach to the selection of controls. The process is likely to involve a number of decision-making steps and internal consultations and discussions. The process should produce an outcome that best suits your enterprise and its business objectives, needs and requirements for the protection of information.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

A small manufacturing business provides products and spare parts through several supply chains. It has a range of different information assets to protect, including those relating to customers, supply chain partners, payment transactions, internal business information and personal information relating to staff.

Based on its risk assessment, the business decides that it must deal with the higher risks, such as the risks to sensitive information, by implementing controls to reduce the risk level. In the case of information assets which are not considered as sensitive, but still essential to its business, the business will outsource the management of the information assets through a risk-sharing scheme.

b) Determine all controls that are necessary to implement the information security risk-treatment option(s) chosen

The selection of controls to reduce identified risks ideally should be a team approach, involving individuals from your enterprise with different areas of knowledge and expertise, for example someone involved with management aspects and someone involved in the day-to-day operations and possibly someone with technical knowledge.

The process of selection can involve several steps:

- Your team should review each individual identified risk and select a security control, or a combination of controls, for each risk.
- The selection should be on the basis of reducing the risk to an acceptable level.
- After selecting an appropriate set of controls, your team should recalculate the risk level in relation to the reduction achieved.
- If the recalculated risk level is not below the level defined as acceptable, then your team should consider further controls.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

- This iterative approach should continue until the desired level of risk acceptance, frequently referred to as the residual risk, is reached. It is important to remember that the level of risk can never be reduced to zero; there will always be a level of residual risk.
- This process is applied to all the identified risks.

There is no single set of controls that can solve all your risk problems. For example, an IT security control is unlikely on its own to solve your risk problems. What is needed is a combination of controls from the following types:

- organizational and management controls;
- people controls;
- operational controls;
- technical controls;
- physical and environmental controls;
- legal and regulatory controls.

This combination of controls is the essence behind establishing and implementing an effective ISMS.

Case study

A small travel booking business provides a range of products and services to customers. It has two travel shops in different towns and uses a range of different information assets which it needs to protect, relating to customers, suppliers of travel services (e.g. airlines, train companies, car hire companies, hotels, currency exchange), payment transactions, internal business information and personal information relating to staff.

In selecting a set of controls to manage its information security risks, the enterprise needs to consider:

- technical controls to secure access to computers processing business information;
- physical security controls to protect unauthorized access to buildings after hours, to offices and physical storage;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

- procedures for staff, with instructions on how carry out their jobs and tasks in a secure manner;
- management security policies;
- legal controls to ensure the information processed is in accordance with legislation, for example to protect personal information, whether it be staff or customer information.

This is a sample of controls; there are likely to be others the enterprise needs to consider.

Sets of controls can be found in industry best-practice and standards, International Standards and other sources. Controls may also be designed as required by your enterprise as best suits your business. These may be a set of controls from a standard modified for your business.

Information security controls should be implemented so they complement each other, so no single control is the solution for all risks. Technical controls need to be supported by management and people controls, and vice versa. Operational controls need to be supported by technical and people controls. A successful and effective approach to reducing risk is to have a suitable combination of controls.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

A primary school (5 to 11-year-olds) already has a number of security controls in place, including: (i) physical security of school gates, buildings and staff offices, and also filing cabinets, and (ii) use of passwords for all school computers used by administration staff, teachers and students. After conducting a risk assessment, the school determines the following additional controls (this list is not comprehensive):

- procedures for the use of the Internet, for example to ensure safe online use and to avoid downloading of undesirable material or malicious software (such as a virus);
- data back-up procedures for all information used and processed by the school;
- procedures on the use of e-mails, including how to protect against the sharing of sensitive school information;
- procedures on the secure use of school laptops by teachers working from home;
- procedures on the protection of personal information;
- staff and teacher awareness of the importance of information security;
- use of anti-virus software and regular updates of the software.

c) Compare the list of necessary controls with those in Annex A of ISO/IEC 27001 to avoid omissions

Annex A of ISO/IEC 27001 is a reference set of information security controls. These are best-practice controls that have been developed and adopted by many businesses across many market sectors and in many countries. These controls have therefore been used and tested in many different business environments. The list is not exhaustive but can be applied to a wide range of security situations. There could be other lists of controls or checklists with a more extensive set of elements, but Annex A of ISO/IEC 27001 is derived from ISO/IEC 27002 and has a proven track record of applicability and international use as a code of best practice.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

The comparison of the necessary controls determined in the risk-assessment process against the content of Annex A is to ensure that no necessary information security controls are overlooked, so the function of this comparison is a control on itself, in case the risk-assessment process is immature or has failed to identify a risk or a necessary control to address it.

There could be controls in Annex A of ISO/IEC 27001 that are unnecessary for an enterprise, according to their activities, technology, people or business type and the information it uses. The determination of the need for a control is the responsibility of the enterprise itself, for example from the results of the risk-assessment process or via the need to comply with contractual or legal obligations.

Case study

A small law firm of 11 staff provides legal advice and help to small businesses has a basic level of security already in place to protect client information. After carrying out a risk assessment it has determined it needs additional controls, in particular to deal with its increased use of the Internet and mobile devices. After comparing its list of controls with those in Annex A of ISO/IEC 27001, the law firm found that some other controls are necessary, such as:

- procedures to cover safe and secure remote working – more work is being carried out away from the office, at home or at the site of a client;
- improved network security for those working remotely and wanting to connect to the information systems in the office;
- improved security awareness and training regarding information security as it applies to their business.

d) Produce a statement of applicability

A statement of applicability is a document that contains the list of controls that you have determined from the process in (b) and the controls resulting from the comparison process in (c). In addition, it should contain justification for why they are included in the statement of applicability, whether they are implemented or not, and the justification for any Annex A controls that are excluded. The document provides a useful record of the results of the risk assessment and treatment processes.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

e) Formulate an information security risk-treatment plan with the risk owner's approval

Your enterprise needs to produce a risk-treatment plan, which should detail how the risk-treatment options have been selected and will be implemented. The plan should include the reasons why specific treatment options have been selected and the benefits your enterprise expects to gain. The plan should also detail the priorities for action to be taken to implement the treatment options, the allocation of the resources needed for implementation and a schedule for the delivery of the implementation.

f) Obtain risk owner's approval of the information security risk-treatment plan and acceptance of the residual information security risks

The risk owners are those people in your enterprise who are accountable for the risks and the overall authority for decisions regarding the management of the risks. They are responsible for approval of the residual levels of risk and the risk-treatment plan.

Subclause 6.2 – Information security objectives and planning to achieve them

This subclause requires the organization to establish a set of information security objectives and specifies several criteria that the organization has to consider and apply when setting each objective.

Guidance

The intent of this subclause is to establish information security objectives that are relevant to the enterprise and aligned to those identified in ISO/IEC 27001, Clause 4 and subclause 6.1.1.

This includes:

- Ensuring the objectives are consistent with the information security policy of your enterprise. This policy should state the commitment and direction of management of your enterprise, and its purpose and objectives in protecting its business and assets from loss of confidentiality, integrity and availability. This objective will help the enterprise minimize any business damage, maximize its business opportunities and investments and ensure the continuity and availability of its business. This type of policy is a high-level management policy and as such it may only be one to three pages long;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

- The objectives being measurable – it is important to take measurements to verify and check that the information security objectives and requirements are being met and that the ISMS remains effective. This may not always be practicable in all cases;
- Ensuring that applicable information security requirements (Clause 4) and the risk assessment (subclause 6.1.2) and risk treatment (subclause 6.1.3) results are taken into account;
- Monitoring, reviewing and updating the objectives as and when necessary;
- Communicating the objectives to all those in your enterprise, especially where they apply to individual job roles, responsibilities and tasks. Communications is an important aspect of information security management, as managers and staff need to be aware and kept up-to-date on information security matters that might affect their work role and the business;
- Documenting the objectives as a record for managers and staff to use, for reference, and assuring compliance.

Your enterprise needs a plan that will outline how it is going to achieve its information security objectives, including:

- Defining **what** needs doing – specific activities and actions to be implemented, roles and responsibilities.
- Determining **what** resources are required to implement the plan, such as personnel, budget and technology.
- Identifying **who** will be responsible for carrying out each task action in the plan.
- Establishing a timeline for **when** each action in the plan will be completed.
- Defining **how** to evaluate the results of the plan and adjust it as necessary to ensure the information security objectives are achieved.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Subclause 6.3 – Planning of changes

This subclause requires the organization to plan any changes to the ISMS, when it considers that it need to make such changes.

Guidance

The intent of this subclause is to plan for changes to the ISMS. Changes are always needed whether they be planned changes your enterprise needs to make, for example adopting a new technology or a new way of doing business, or unplanned changes not under its control, for example supply chain changes, new legislation or a security incident that needs changes or improvements to your system. For both these types of change you need to consider your information security in how your enterprise will adapt or respond to the change. You need to consider your current information security and what needs to be done to your information security to maintain or improve its effectiveness.

When a change or changes have been identified you need to determine how the change fits into your business environment and your business operations, making sure the changes work for your enterprise and that there are no conflicts. You should check that the changes do not introduce any additional risks or impacts and, if they do, how you are going to address these. You need to make sure there is sufficient awareness and training of staff with respect to these changes, including information security training. You should communicate all changes to interested parties where appropriate, for example business partners.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

A small warehousing and storage company proposed to upgrade all its IT and introduce more automation in its storage facilities. These changes could introduce new information security risks and so the company needed to reassess its risks and decide on an appropriate set of controls to manage those risks that are above the level of acceptance. Also, the company needed to update its information security policies and procedures to take account of these changes, and provide training and awareness in the use of the new IT. The changes may have an impact on existing operations and business practices, which may be related to information security. These changes could have an impact on the legal and regulatory requirements, therefore any non-compliance issues need assessing. The company would have to discuss any implications with staff, for example, the introduction of automation, and gain support from staff for these changes.

After your enterprise has approved a proposal, then its implementation needs to be carried out in a planned and controlled manner to avoid any disruption and system failures from the old IT to the new IT. This should involve some form of testing and validating the new technology before its use in day-to-day business operations. Also it is useful to monitor and review the changes to check their effectiveness and that they do not introduce any new risks or vulnerabilities.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

7. Support

This Section consists of five subclauses, with subclause 7.5 consisting of three further subclauses, covering the following aspects:

Subclause 7.1 – Resources

The organization has to provide the necessary resources to establish, implement, monitor, review and continually improve the ISMS.

Guidance

The intent of this subclause is for the enterprise to determine and allocate the resources it needs for its ISMS. The term resources can apply to people, infrastructure, technology, budgets, physical equipment, buildings and offices. ISO/IEC 27001, subclause 7.1 is about the determination and provision of resources specifically for the establishment, implementation, maintenance and continual improvement of the ISMS.

It is important that your enterprise has the right types of people resources for the work that has to be done. Your enterprise needs staff with the right competence, for example customer services needs staff who can deal with customers and technical support needs staff who have technical knowledge and skills to resolve technical problems, and the same applies to information security management. ISO/IEC 27001 does not require that the roles and responsibilities for information security management be full-time jobs or tasks. What is required is that roles and responsibilities are clearly defined and that they are carried out as and when needed. The types of resources required for the information security management may need to be dedicated to specific information security management tasks and some may be related

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

to general tasks undertaken by staff. The staff time the enterprise allows for carrying out these roles and responsibilities is for the enterprise to decide, and staff time is likely to be needed to carry out other tasks and work assignments unrelated to information security management.

Case study

A small transport business provides transport services for schools, airports and hospitals. The business decides to consider the resources needed in the following areas:

- information security policy, procedures, reviews, monitoring and improvements;
- information risk management;
- information security auditing;
- IT security;
- physical security.

Determining what resources will be needed includes identifying the necessary budget and whether internal staff have the competences to cover most of these areas. If not, then external support will ne be required.

Subclause 7.2 – Competence

ISO defines competence as the ability to apply knowledge and skills to achieve intended results. This subclause specifies four specific requirements for an organization to demonstrate competence for staff involved in establishing, implementing, operating and maintaining the ISMS.

Guidance

The intent of this subclause is to determine the required competence for the jobs, tasks or activities in your enterprise for its ISMS. The objective is to ensure that the managers and staff carrying out those jobs or activities are competent to perform them. The definition of competence is the ability to do something successfully or efficiently. This requires certain skills, knowledge and expertise, and other things that could support competence.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

For example, someone engaged in risk assessment should have knowledge and expertise in the principles of risk and related topics, the relationship to information security management, how to engage with management and risk owners on risk acceptance and risk-assessment criteria, how to undertake the identification, analysis and evaluation of risk, how to engage and communicate with other staff to discuss risks related to the business of the enterprise and how to produce risk assessment documentation.

Once your enterprise has determined what types of competencies are required, it should consider its existing staff and their skills, work experience, education and training in information security management. Where there is a gap between what is needed and what is available, the enterprise needs to determine how it is going to fill this gap and to take the necessary action. It may be that some training is required, more work experience is required or external help is required on a short-term basis.

It is important to note that being educated and having qualifications does not mean you are competent. Having the ability to do something correctly, efficiently and effectively is competence. Work experience, practical knowledge and skill in doing a job is highly relevant and essential to having competence; at the same time having education and training is important support for gaining knowledge.

It is important to check to see whether actions taken to acquire the skills and experience necessary to support the ISMS have been effective. If any gaps between the competence you have available and the competence you need remain, you can then make sure they are addressed. For example, if a staff member has done a course in information security management and has now taken on a new role relevant to the ISMS, it is important for this staff member to be able to gain practical work experience in applying the knowledge gained during the course.

Competence requirements will change over time, so it will be necessary to conduct periodic reviews of existing competence and new requirements and to take action to address any gaps that are identified.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Case study

The owner of a one-person IT consultancy business has an ISMS. This director has significant experience helping other organizations develop, run and improve their ISMSs, and has experience managing the technical controls, physical controls and organizational controls. The director also subscribes to a service that provides regular information security threat intelligence updates and spends time each week keeping their knowledge up-to-date. The director has a professional network of experts who can provide further information or expertise if needed.

Case study

A family-owned bakery and patisserie with five outlets in different towns has adopted an ISMS approach across the whole of its business. One of the family members has a technology background and this has led to the adoption of good IT security practices for the enterprise. The business does, however, need to gain staff competence in the management aspects of using the ISMS. Some staff have been given in-house awareness training to increase their competence with respect to information security management, and some have been given specific roles and responsibilities.

Subclause 7.3 – Awareness

This subclause requires that all people working under the control of the organization shall be aware of the information security policy, their contribution to the ISMS, and the consequences of not conforming with the requirements of the ISMS.

Guidance

The intent of this subclause is to ensure that staff in your enterprise are aware of the information security policy, relevant information security objectives, their contribution to the effectiveness of your ISMS and the implications of not conforming with ISMS requirements.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001:2022

All staff working for the enterprise should be made aware of the information security risks and have sufficient understanding of these risks and their consequences, to support the information security policy and to be able to undertake their work activities. An important aspect of awareness is for all staff to understand their own contribution to information security management and be aware that this contribution is essential to the overall effectiveness of information security management.

Staff should participate in some general information security awareness training as part of their induction when they join the enterprise. On-the-job awareness training can also take place, which can be specific to the job function of the individual. In addition, annual refresher awareness training might also be given to make sure staff are up-to-date with any new developments related to the information security management policies and procedures within the enterprise and as a reminder of existing information security management procedures.

All your enterprise staff should also make sure that they aware of the implications of not following the ISMS requirements. For example, nonconformity problems start with people not following the information security policy or procedures, and this can lead to consequences that result in harm or damage to the enterprise, which affects all staff. As mentioned in Clause 6, the consequences of a breach of security could lead to theft of information, loss of confidentiality, integrity or availability of information, loss of business, legal actions or damage to image and reputation. Depending on the severity of the nonconformity, the enterprise needs to take action that is proportionate to the degree of nonconformity. For example, this may be a warning in the less severe cases through to disciplinary action or termination for the critically severe cases. The enterprise may decide what action to take in line with its own internal rules on discipline.

Subclause 7.4 – Communication

This subclause requires the organization to determine the needs for internal and external communications for the ISMS, specifically on what, when, with whom and how to communicate.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Guidance

The intent of this subclause is to establish the internal and external communications your enterprise needs and which are relevant to your ISMS.

Communications are essential to the overall success of the ISMS. If only one or two staff understand the importance, relevance and role of the ISMS, then this is of no use to the enterprise. At all management and staff levels in the enterprise, there needs to be sufficient communication about the ISMS. For example, the information security policy needs to be communicated to everyone, understood and applied by everyone. Procedures dealing with IT access, back-ups, protection of sensitive information, reporting security incidents, physical access, visitor access and other activities need to be communicated to and known by all staff.

The enterprise needs to decide what needs to be communicated and to whom, for example what needs to be communicated to staff and what needs to be communicated to external parties. Enterprise policies and procedures and their updates need to be communicated to all staff.

Information on security incidents that may affect the enterprise need to be communicated to all staff where they are generally applicable and to some staff where the incident may impact their area of work. Reporting of incidents needs to be communicated to all relevant people. A serious breach of security of a criminal nature should be communicated to law enforcement authorities, and where it may affect business partners, suppliers or customers. Likewise, external parties might communicate incidents affecting their business to you if the incident is likely to have an impact on your enterprise.

How you communicate is a decision for your enterprise. For example, you might decide to have staff meetings, to use e-mails, newsletters, internal notices or reports or other means of communicating with staff. Depending on the urgency of the communication, such as an incident that requires immediate action, then the communication might be phoning the relevant persons.

Communications should be documented or recorded, especially in the case of a security incident, as this provides evidence of what was communicated, when it was communicated and to whom it was communicated.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Example

It may be helpful to create a table with each of the interested parties listed in the first column and the information about what to communicate, when, with whom and how as subsequent columns, so that this information is specific to each interested party. However, you decide to document this information, it should be made available to those persons in the enterprise responsible for communicating with the different internal and external interested parties.

Subclause 7.5 – Documented information

This subclause is in three parts, covering: general requirements; creating and updating documented information, and; the control of documented information. The subclauses are:

7.5.1 General

7.5.2 Creating and updating

7.5.3 Control of documented information

7.5.1 General requirements

This subclause requires the organization to have documented information that is appropriate to the scale of its ISMS, its complexity, size of the organization, and competences of its staff.

Guidance

The intent of this subclause is to ensure that your enterprise controls the documented information needed for conformity to the requirements of ISO/IEC 27001, as needed for the effectiveness of your ISMS (see ISO/IEC 27001, subclause 4.4.2). For example, documented policies and procedures, risk assessment and risk-treatment results, management reports, audit reports and performance records.

The following are some specific examples required by ISO/IEC 27001 – the numbers in parentheses represent the applicable clauses of the standard:

- the information security policy (5.2);
- information about the risk-assessment process for information security (6.1.2);

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

- statement of applicability (6.1.3);
- records of approval by risk owners, of the information security risk-treatment plan and acceptance of the residual information security risks (6.1.3);
- documented evidence of the competence of people doing work under the control of the organization (7.2);
- information to provide confidence that processes to meet information security requirements are carried out (8.1);
- the results of information security risk assessments (8.2);
- the results of the information security risk treatment (8.3);
- monitoring and measurement results (9.1);
- audit programme(s) and the audit results (9.2);
- results of management reviews (9.3);
- nonconformities identified and any subsequent actions taken (10.2);
- records of any corrective action (10.2).

ISO/IEC 27001 is not prescriptive in terms of the content or extent of documented information needed. This will vary from one enterprise to another according to their size and the complexity of their business, operations and processes, and the customer, statutory and regulatory requirements. For example, documented information for a small transport business will be simpler and less extensive than that of a much larger enterprise. The latter might have more external requirements and whose document information needs to cover more complex business operations.

To make sure that the ISMS reflects the needs of your enterprise and helps in making it as effective as possible, there will need to be documented information to ensure consistency and visibility of what is being done to support information security, by whom and how.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

7.5.2 Creating and updating documented information

This subclause requires the organization to have appropriate formats, identification, review and approval processes, when creating documented information.

Guidance

The intent of this subclause is to ensure that when you create and update documented information for your ISMS you have used appropriate identification, format and media, and that this is reviewed and approved.

Documented information needs to have some form of identification, for example, title, date, author/document owner or reference number (used in some combination that is appropriate to your enterprise). This will enable your enterprise to determine the information and its current status.

Additionally, your enterprise needs to decide on an appropriate format and media for documented information; for example, hard copies, electronic formats or both. If electronic versions are used then your enterprise needs to make sure that all staff are using the same software version for creating and updating documented information.

Your enterprise needs to have a process for the review and approval of documented information, and someone in the enterprise should be given the authority of approving documented information.

7.5.3 Control of documented information

This subclause is highly prescriptive with several detailed requirements for controlling documented information. This is to ensure that applicable staff and external stakeholders are provided with, or have access to relevant documented information that is up-to-date.

Guidance

The intent of this subclause is to ensure that documented information is available in a suitable format and medium whenever needed. Additionally, it needs to be adequately protected to ensure its confidentiality, integrity and availability are maintained.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Documented information needs to be available to all those that need access to such information and this may include externally interested parties. The documented information needs to be in a form that is appropriate for its use. Documented information in electronic form is much easier to use and share, which is helpful to external parties and your staff that work remotely. It is important that there are suitable controls in place, including for the distribution of, protection of and access to documented information. Your enterprise needs to ensure controls are in place to protect against information loss, improper use, unintended changes and loss of confidentiality.

In order to make sure that your documented information remains up-to-date, complete and relevant over time, these documents should be given a review date. Your organization should then validate that its documented information has been reviewed and approved within that time frame, for example annually or within two years. This is important because the organization will change over time and the information in these documents can become out-of-date, which can lead staff to either not trust the documented information or to follow out-of-date procedures or guidelines.

Information has different levels of sensitivity or confidentiality and criticality. For example, financial records or personal information about employees would generally be considered more confidential or sensitive than publicly advertised information about a product or service. There are many ways of classifying information, including for public use (not sensitive), internal only, and confidential or restricted, which are only accessible to specific individuals in the enterprise, for example financial information, human resources information or information that gives your enterprise competitive advantage, such as information about product development.

Your enterprise should determine how and where documents with different levels of sensitivity or confidentiality are made available. For example, information you are happy for everyone to see about your products or services can be made available on your Website or posted on the wall of your shop. Documents for internal use can be made available in your organization's electronic document repository or in a filing cabinet. Restricted documents are documents that should only be made available to the specific individuals or teams that are allowed to view them, for example, finance information only made available to the finance team or information about information security incidents only made available to the security operations team.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

It is possible to allow some information to be made available for some people to read but not make changes to that information. Consideration should be given to how and when access to certain documents may be needed. For example, if the business continuity plan that explains what to do if there is a disaster is only available electronically on a system that is brought down by a disaster, it cannot be accessed and used, so it may be necessary to store a hard copy offline or have access to printed copies of some documents.

Documents should be controlled so that only the people allowed to see them are given access to them, people are prevented from making unauthorized changes and they are prevented from sharing documents with anyone not authorized to see them.

Certain types of documented information may need to be protected by encryption when it is transferred from one party or location to another, for example via e-mail, or when it is stored.

It may be helpful for your organization to list what documents or document types should be distributed to whom, so it is clear who should have access to what information. Your enterprise can then organize the distribution of documents by document type or by who will be receiving it, as well as the date distributed. Where possible, information should only be visible to those with a need to view or use it. For example, your enterprise can allow only specific people to see or open specific file folders or documents.

As regards storing and preserving documents, there are a number of considerations. Documents can be securely stored at another location or in the cloud and either physically or virtually transferred to another location to ensure preservation. Some enterprises digitise their printed documents so they can be made more easily accessible. Archived documents should retain relevant access controls information so that even once the document is archived it is still always clear who is allowed to see it.

Your enterprise should have a defined process for managing changes to documents and version control. This process should be applied in a consistent way, so that there is clarity about what constitutes a complete version change (e.g. from version 1 to version 2) as opposed to a partial version change (e.g. from version 1.1 to 1.2). Approvals of new versions of documents should also be carried out in a timely way so that new versions are not prevented from being used for months while approval from a senior executive is pending. The organization should consider how and when to

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

alert staff and other relevant persons about new versions of documents, for example the latest version of a policy.

Different types of information, for example financial information or information that includes personally identifiable information about employees or clients, can have different required retention periods. These retention periods are often required in accordance with legal, regulatory or statutory requirements and contractual obligations, so it is essential to understand what these retention periods are and adhere to them.

Your enterprise should determine what the different retention periods for different document types are and document these so that there is clarity about the required retention period for each document type. Regular reviews should then be done to ensure that your enterprise is retaining documents in alignment with the documented retention periods. Your enterprise should also determine the final disposition of documents at the end of their retention period, which means whether they will be destroyed, archived, provided to another party, etc.

Your enterprise should ensure that documents remain legible throughout their retention period. For example, ensuring that a document can be read by available software or, if printed, that the printed copy is complete and readable.

It can be useful to create a common template for all internal documents that ensures classification markings are always included and visible. For example, the footer of the document can include something that says Internal Use Only or Commercial in Confidence for different document types. Determining location and access to internal documents can be easily defined. Retention periods for internal documents can also be defined and managed. Documents of external origin that are necessary for the planning and operation of the ISMS, for example a performance report from a supplier that lists potential information security vulnerabilities, also require a consistent process to ensure that there is clarity about classification, access, storage, retention and other considerations regarding these documents.

Some organizations collect, register and manage documents of external origin, such as reports from suppliers or proposals from customers, in the same way they manage internal documents. For example, the organization may add a cover sheet with relevant classification markings to show the level of sensitivity, required retention period and other relevant data and

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

include it in the same document management system used for internal documents. Other organizations use a separate process to store and manage documents of external origin, for example International Standards, which may have copyright requirements or contain customer data, which can have confidentiality, privacy or other contractual considerations.

8. Operations

This clause consists of three subclauses, which are:

8.1 Operational planning and control

8.2 Information security risk assessment

8.3 Information security risk treatment

Subclause 8.1 – Operational planning and control

This subclause requires the organization to plan, implement and control the processes required to meet the objectives of the ISMS, and manage the risks identified under Clause 6, Planning, in ISO/IEC 27001.

Guidance

The intent of this clause is to ensure that you plan, implement and control the processes that are needed for your ISMS. Risks and opportunities are determined during the planning stage in Clause 6, for planning.

Your enterprise needs to have a plan of action for the implementation and control of the processes according to the criteria for the processes needed to meet the requirements and actions determined in Clause 6. Depending on the size and complexity of your enterprise, you should determine what resources are needed and if the current set of resources is sufficient. The controls needed should confirm that criteria are met, ensure the objectives of the ISMS are met and determine where improvements are needed.

The risk-assessment process described under Clause 6 will result in a set of risks prioritized for action and documented in a risk register, according to the severity of these risks. The planning process in turn will determine which control techniques and tools are required for each risk. Therefore, your

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

enterprise will need a plan to apply each of the applicable control techniques and tools in a systematic and controlled manner.

Additionally, establish the necessary activities to control planned changes to the information security processes. This includes changes to the processes themselves and changes to the criteria and rules used to evaluate the processes and should be aligned with the actions to fulfil the requirements described in subclause 6.3 of ISO/IEC 27001.

Review unintended changes and the consequences of such changes to the information security processes, taking action to mitigate any adverse effects. This includes identifying and mitigating any potential risks that may arise as a result of unintended changes to the ISMS, its context, policies, roles and responsibilities and the ability to achieve the objectives established.

Ensure externally provided processes, products or services that are relevant to the ISMS are controlled. This includes ensuring that these processes comply with the rules established for the enterprise's internal processes.

Subclause 8.2 – Information security risk assessment

This subclause requires the organization to perform periodic risk assessments, either at planned intervals, or when there are significant changes that in turn result in changes to the ISMS.

Guidance

Your enterprise needs to perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established through applying subclause 6.1.2 of ISO/IEC 27001. Conducting regular information security risk assessments is an important and essential activity to ensure your ISMS is up-to-date and effective.

There are many different types of change that will need a review of the risks. For example, changes to the needs and requirements of interested parties as discussed and determined in Clause 4. Your enterprise may introduce new technologies or change the way it does business, such as using more online transactions and processing. It might change its service provider or use new services, and the level of security threat might change. All these may introduce new risks and consequences in your business. Reassessing your

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

risks is therefore necessary to make sure your ISMS is still able to control the risks it faces.

The frequency of these assessments will depend on the size and complexity of your enterprise, the type of information being protected and the level of risk associated with the information and the technology used to store, transmit and process it. There is no defined period of when to do a risk assessment, it is for your enterprise to decide the frequency. Your enterprise needs to determine, for example, whether a yearly risk assessment is needed or whether the period should be shorter or longer.

Outside of this defined period there will always be cases that may require a risk assessment when significant changes have been made or when a serious security incident has occurred.

As discussed in the section of this handbook for Clause 6, you need to identify and prioritize risks for information security, taking into account their likelihood and impact. Include in this assessment the current controls and actions to mitigate these risks and evaluate their effectiveness.

Document the results of the information security risk assessments. This documentation should include the risks identified, the likelihood and impact of these risks, the current controls in place and any additional controls determined to address these risks.

Review and update the results of the information security risk assessments regularly to ensure that the risks for information security are being effectively managed. This may include updating the risk-treatment plan and implementing additional controls as necessary.

By conducting regular information security risk assessments, an enterprise can ensure it is effectively managing information security risks and protecting its information assets. This documented information on the results of the assessments is also a valuable resource for understanding the information security risks and the actions taken to mitigate these risks.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Subclause 8.3 – Information security risk treatment

This subclause requires the organization to implement the information security risk-treatment plan and then document the results of the risk treatment for information security.

Guidance

The information security risk treatment plan created by applying subclause 6.1.3 e) of ISO/IEC 27001 should be implemented. Your enterprise should assign sufficient resources for the implementation. The purpose of the risk-treatment plan is to address the risks identified in the risk-assessment process; in most cases this would mean reducing the risk by controls that modify the likelihood of an event or reducing the impact on assets. Your risk-treatment plan needs to be approved by relevant decision-makers and risk owners to ensure it aligns with the enterprise's business objectives and the risk management process established.

The treatment plan should include risks and their impact and likelihood, level of risk, treatment options for each unacceptable risk, necessary controls, responsibilities for implementing specific controls and the activities for appropriate individuals or teams.

There should be a timeline for implementing the plan that considers the availability of resources and the activities that depend on others involved in the implementation.

Monitor and track the implementation of the plan, considering if the timeline is met, if the resources are sufficient and if staff are competent enough to carry out the activities and implement the controls.

Your enterprise should retain documented information of the results of implementing the information security risk treatment, including any changes made to the risk treatment plan, the status of implementation and any residual risks that remain. This should also include evidence of the implementation of controls and any residual risks. This documentation should be available for review by relevant decision-makers and auditors.

Review the results of the information security risk treatment and update the risk-treatment plan as necessary to reflect changes in the enterprise's risk profile or business objectives.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

9. Performance evaluation

This clause describes the requirements for evaluating the effectiveness of the ISMS and consists of three subclauses, which are:

9.1 Monitoring, measurement, analysis and evaluation

9.2 Internal audit

9.3 Management review

Subclauses 9.2 and 9.3 each consists of further subclauses.

Subclause 9.1 – Monitoring, measurement, analysis and evaluation

This subclause requires the organization to determine what to monitor, when, how and where, including provisions for analysis and review of the results of monitoring.

Guidance

The intent of this clause is for your enterprise to determine what processes for measuring and monitoring are required, when to perform these processes, who is responsible for them and how to carry out the analysis and evaluation of the results of these activities.

Subclause 9.1 of ISO/IEC 27001 is highly prescriptive in that it states in five parts exactly what an enterprise needs to do.

Subclause 9.1 a) – what needs to be monitored and when: The top management should first explain what will be convincing evidence that the information security management system is meeting its objectives (clause 5.2 b)). For example, failure to meet an objective such as there should be no inappropriate disclosure of personal information, could result in an incident, such as the loss of a laptop. An appropriate measure in this case is the number of incidents. The enterprise owner might also want other information such as whether risk assessments and meetings are being conducted as scheduled.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

In some cases, measurements are made over a period. ISO/IEC 27001 refers to such a series of measurements as monitoring.

Subclause 9.1 b) – methods for monitoring, measurement, analysis and evaluation: Measurements can be simple numeric values, such as numbers of people who attended an event or the number of incidents. They can be ratios, such as the number of people who attended divided by the number of invitees, or a more complex formula. Regardless of the methodology, it should be defined for all measures before the corresponding measurements are made.

Care should be taken when making quantitative measurements to avoid measurement errors. One might, for example, take the average of several measurements. Care should also be taken when making qualitative measurements to avoid subjectivity. Such errors can be reduced by giving instructions for the assignment of values. For example, poor means a score of less than 10%.

Subclause 9.1 c) – when to perform the monitoring and measuring: the times and frequencies at which measurements are made can be different for different measures. For example, measurements for one activity might be made once a month, whereas another might be made annually.

Subclause 9.1 d) – who performs the monitoring and measuring: this process should be assigned to individuals, while management may decide who this is.

Subclause 9.1 e) – when to analyse and evaluate the results of monitoring and measuring: the schedule for analysis and evaluation should be determined by criticality of the process being measured and monitored. For example, is it data that will inform immediate action? Otherwise, it is not always necessary to analyse and evaluate the results as soon as measurements are made. In some cases, it is preferable to make a series of measurements and then analyse the results.

Subclause 9.1 f) – who analyses and evaluates the results of monitoring and measuring: different skill sets can be required for measuring, analysis and evaluation. Such differences should be borne in mind when allocating responsibility for analysis and evaluation.

While it is useful for the business to write down plans for monitoring and measuring, the measures, formulae, timings, who does what and when, the standard places the emphasis on the results. It is these that will inform the business as to whether the ISMS is meeting its objectives.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Subclause 9.2 – Internal audit

This clause consists of two further subclauses, which are:

9.2.1 General

9.2.2 Internal audit programme

Subclause 9.2.1 – General

This subclause specifies that the organization must perform internal audits at intervals to provide information on whether the ISMS is effective, maintained and conforms to the requirements of ISO/IEC 27001.

Guidance

The intent of this clause is for your enterprise to gain information through conducting internal audits about the performance and effectiveness of your ISMS. An internal audit should be an impartial view of whether your ISMS has been effectively implemented and maintained. This audit is used to determine whether your ISMS conforms to the requirements of ISO/IEC 27001 as well as the requirements of the enterprise.

Case study

An online florist business conducts internal audits on a yearly basis. However, it has recently experienced several security incidents that have disrupted the business, resulting in a medium level of impact. The enterprise then decides to conduct an internal audit to determine whether the ISMS is still effective and operating as expected. The enterprise's management aim to determine the cause of the disruptions, thus enabling management and risk owners to make appropriate improvements.

Case study

The reception staff in a health clinic have daily contact with patients and take the opportunity to get feedback on whether the patients are satisfied with the service they receive. After collecting the feedback, the staff note the suggestions and share these in staff meetings.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Subclause 9.2.1 – Internal audit programme

This subclause specifies the requirements for planning, establishing, applying and maintaining an internal audit programme.

Guidance

Your enterprise needs to establish, implement and maintain an audit programme. The programme should set up a series of audits for a specific time frame. This should include how frequently an audit should be carried out (e.g. monthly, quarterly, yearly). The audit programme should define the methods to be used, which might include observation of the ISMS in operation, interviews with relevant staff, sampling of processes in place and examination of documented information.

When assigning staff to undertake the audits, your enterprise needs to ensure objectivity and impartiality during the audit process. In general, a member of staff should not audit their own work.

Your enterprise should determine the scope of each audit and the audit criteria to be used. The scope might specify areas of the business, processes or activities. The criteria might include specific standards to be used, specific requirements to be checked or when corrective action is needed and the time frame for making corrections and improvements. An internal audit is a good opportunity for observing weaknesses and areas for improvement.

The audit should result in an audit report detailing the findings of the audit, evidence of nonconformity, areas for correction and improvement. This report is needed as input to the management review, which is described in the next section.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Subclause 9.3 – Management review

This subclause is divided into three further subclauses, which are:

9.3.1 General

9.3.2 Manage review inputs

9.3.3 Management review results

Guidance

The intent of this clause is to ensure that your enterprise conducts management reviews.

The purpose of the review is to check that your ISMS is:

- suitable – does it still fulfil its purpose?
- adequate – is it still sufficient?
- effective – does it still achieve the intended results?

The enterprise's management should review the ISMS at planned intervals to ensure that it is working as intended. Reviews can take place at intervals defined by management, although comprehensive management reviews are typically at annual intervals, while more complex organizations often have smaller reviews more frequently, e.g. once per month or every quarter.

This management review can be stand-alone or in combination with other management review meetings. For example, they could be carried out weekly, monthly or around the same time that management has other meetings, for example business planning, strategic planning or operational meetings. This can add value and avoid redundant multiple meetings.

The review meetings will have a number of inputs to consider:

- Actions decided upon at previous meetings need to implemented. Reviewing the status of actions from previous review meetings is therefore an important first step as in any formal meeting with minutes.
- External and internal issues, for example changes to the market in which the business operates and world events, can affect the ISMS. Such changes can modify the likelihood of cyber-attacks; also, changes in the law can affect what businesses must do to preserve the security and privacy of information. There can be internal changes, such as staff

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

turnover, response to new business opportunities and adoption of new technologies, that affect the ISMS.

- Customers can also have new requirements that can affect the ISMS.
- The results of measurements and audits provide information concerning how well the ISMS is meeting its objectives. Nonconformities, especially repetitious nonconformities, can highlight areas of weakness where improvements can be desirable.
- Comments from customers and staff can also identify areas of the ISMS where improvements can be made.
- Risks are forever changing, which is why risk assessments must be conducted at planned intervals and when significant changes are proposed or occur. Such changes can necessitate a change in the information security controls that are used to mitigate risk. Because such changes affect the ISMS, it is important to include them in the management review.
- Management is committed to continual improvement and the review meeting is a good time to demonstrate that commitment.

The most important outputs of a management review concern opportunities for improvements and changes that are to be made to the ISMS.

The management review minutes serve as a permanent record of the review meeting and the decisions taken.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

10. Improvement

There are two subclauses to this final clause, which are:

10.1 Continual improvement

10.2 Nonconformity and corrective action

Subclause 10.1 – Continual improvement

An enterprise has to implement a continuous improvement process to ensure the suitability, adequacy and effectiveness of its ISMS.

Guidance

The aim of this subclause is to ensure that your enterprise identifies opportunities for improvement of your ISMS. Improvements can help your enterprise keep its ISMS up-to-date, improving the performance and effectiveness, correcting or preventing undesirable effects of risks and their consequences, and meeting the needs and requirements of interested parties.

Improvements might be identified through different methods, for example:

- results of risk assessments (Clauses 6 and 8 of ISO/IEC 27001), security incident activities and reports of emerging threats that might have a potential impact on the enterprise;
- actions resulting from monitoring, internal audit and review activities (Clause 9 of ISO/IEC 27001);
- actions to avoid recurrence of nonconformities (Subclause 10.2 of ISO/IEC 27001);
- feedback from management, staff and other interested parties;
- changes due to the introduction of new business processes and technologies.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022

Improvements should be carried out to ensure that your ISMS continues to be effective, appropriate and suitable for your enterprise and the protection of its information. Improvements will be necessary over a period of time to ensure all changes that affect your enterprise are considered from a risk and impact point of view.

Case study

A small architectural practice is highly dependent on the use of technology to produce designs for buildings, offices and houses, and to communicate with its customers on design specifications. It periodically reviews its needs and requirements for information security, taking account of feedback and reports on current and emerging risks, and its current information security controls and the performance and effectiveness of those controls. It has regular monthly meetings with staff to discuss any security related issues encountered in order to identify any opportunities for improvement.

Subclause 10.2 – Nonconformity and corrective action

This subclause requires the enterprise to identify nonconformities, respond to them, analyse the root causes, and then take steps to either minimize the chances of a recurrence of the nonconformity, or to eliminate them happening again if possible.

Guidance

The intent of this subclause is to ensure that your enterprise manages any nonconformities it has identified and that it takes appropriate corrective action to address the nonconformities.

A nonconformity is a failure to conform with the requirements given in ISO/IEC 27001; this can include issues related to these requirements, such as non-compliance with statutory or regulatory requirements, breach of contractual obligations, breach of information security policy or problems arising from external interested parties. Your enterprise should take the necessary action to investigate what has gone wrong and the causes of the problem, correct the problems and prevent any future recurrence. Your enterprise should seek to eliminate the causes and effects of the problem.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 27001 :2022