Small Business Standards

European DIGITAL SME Alliance

SME GUIDE:

IMPLEMENTATION OF ISO/IEC 27001:2022 ON INFORMATION SECURITY MANAGEMENT

NOVEMBER 2025

CONTENTS

FOREWORD

In the framework of the EU-funded actions for support to SMEs in standardisation by SBS, the European DIGITAL SME Alliance developed and now upgraded an SME Guide for the implementation of ISO/IEC 27001 on information security management.

The main goal of the Guide on information security management is to support SMEs in understanding and applying ISO/IEC 27001 for information security management systems. With the publication of the 2022 revision of the standard, an update was necessary to reflect the new requirements and adapt the content to the European cybersecurity landscape. The new edition of the Guide continues to provide SMEs with a practical and accessible tool to strengthen their information security management in line with international standards.

This publication is a result of the efforts of the DIGITAL SME "WG27K" working group, which brought together experts familiar with standardization issues for information security management systems. These activities were coordinated by Guido Sabatini and chaired by Fabio Guasconi. The recent updates have been led by Davide Iaccarino, Cybersecurity & Data Project Manager at the European DIGITAL SME Alliance, in collaboration with Davide Giribaldi, a cybersecurity and standardisation expert and one of the original co-authors of the guide. Contributions to the Guide were provided by experts with strong knowledge of information security and standardization, including Georgia Papadopoulou, George I. Sharkov, David Bulavrishvili, Sergio Oteiza, Holger Berens, Ermal Çifligu, Sebastiano Toffaletti, Nanuli Chkhaidze, Yuri V. Metchev, Thorsten Dombach, and Alexander Häußler.

Disclaimer: this Guide is informative in its contents. Implementing this Guide does not imply full compliance with ISO/IEC 27001. This document is not intended and cannot be used as a substitute for certification according to ISO/IEC 27001. This Guide only reflects Small Business Standards' and European DIGITAL SME Alliance's views. The European Commission and the EFTA Member States are not responsible for any use that may be made of the information it contains.

European DIGITAL SME Alliance is the largest European network of ICT small and medium-sized enterprises (SMEs), representing around 45,000 tech SMEs.

Rue Marie Thérèse 21, 1000 Brussels, Belgium

office@digitalsme.eu

www.digitalsme.eu

T +32(0)2 893 02 35

Transp. Register 082698126468-52

Small Business Standards (SBS) is the European association that represents small and medium-sized enterprises' (SMEs) interests in the standardisation process at both European and international level.

Rue Jacques de Lalaing 4, 1000 Brussels, Belgium

info@sbs-sme.eu

www.sbs-sme.eu

T +32(0)2 285 07 27

Transp. Register 653009713663-08

Co-financed by the European Union and EFTA

GLOSSARY

To better understand this Guide, here are definitions of the most common and specific terms:

Asset: Any item that has value to the organisation. There are many types of assets, e.g. data, hardware, software, service providers, personnel, and physical locations.

Attack: Deliberate form of endangerment, e.g. an unwanted or unjustified act with the aim of gaining advantages or harming a third party through action on a set of assets.

Availability: Property of being accessible and usable upon demand by an authorised entity.

Confidentiality: Property that makes information available or disclosed only to authorised individuals, entities or processes.

Control: A measure to modify risk. Controls include processes, policies, devices, practices, or other actions which can effectively modify risk.

Integrity: Property of accuracy and completeness.

Information security: Preservation of confidentiality, integrity and availability of information.

Risk (information security): An information security risk with the potential that threats will exploit the vulnerabilities of an information asset and thereby cause harm to an organisation.

Risk assessment (information security): Overall process of risk identification, risk analysis and risk evaluation.

Risk treatment (information security): Process to modify risk – usually involving risk avoidance, risk sharing, risk mitigation or risk acceptance.

Threat: Potential cause of an unwanted incident, which may result in harm.

Vulnerability: Weakness of an asset or control that can be exploited by one or more threats.

1. INTRODUCTION TO CYBERSECURITY

Nowadays, information is one of the main assets for most organisations, and for many - it is the foundation of their value creation. Others rely heavily on processing information to support their business operations.

Yet the threat landscape has become more complex, with attackers using advanced and persistent methods to exploit this dependency. We have indeed witnessed many examples of their illegal behaviour, such as viral ransomware attacks (WannaCry, Petya), leaks of personal data from large corporations (e.g. Equifax, Marriot), leaks of intelligence agencies' spying tools, and even breaches affecting critical infrastructure such as the Colonial Pipeline incident.

As the number of threats increases and risks grow, organisations are expected to adopt a proactive resilience-based approach to managing information, for example by adopting these simple protection measures:

- implementing password access to computers and systems;
- installing antivirus software on end-user workstations and server environments;
- disabling USB flash drives within the organisation; or
- acquiring more advanced and costly solutions.

While many of these measures are effective in protecting systems, others are a pure waste of financial and human resources. This is not because the above-mentioned tools are bad or inefficient. The main problems here are deciding which tools to select and figuring out how much they cost and how to implement them effectively for each organisation's business.

WHY A GUIDE FOR SMALL AND MEDIUM-SIZED ENTERPRISES (SMEs)?

- SMEs make up the majority of businesses in Europe, outnumbering large corporations and employing more people. They are recognised to be a driver for innovation in Europe.
- Most SMEs underestimate their risk level for cyber-attacks, in the belief that they do not handle any information worth stealing.
- However, small businesses have a lot of digital assets compared to an individual user and they often have fewer security measures in place than large organisations.

Due to the growing complexity of today's digital environment and the interdependencies of information flows, many organisations recognise the need for dedicated roles such as information security managers, cybersecurity professionals, and governance committees. Increasingly, specific teams or departments are also being set up for incident response and resilience. However, uncertainty remains in many organisations about whether their investments in security measures provide sufficient value. Weaknesses in cybersecurity can still result in significant issues, which can be mainly assigned to three categories:

- loss of availability, impeding business activities;
- loss of confidentiality, causing damage to the reputation of the organisation or even legal action;
- loss of integrity, leading to the use of incorrect or even falsified data.

Cybersecurity is key to protecting the assets of businesses of every type and size. But what exactly is cybersecurity?

1.1 CYBERSECURITY DEFINITION

There is no formal definition for **cybersecurity**, but its meaning is similar to information security. Cybersecurity is often considered to include the most technical aspects of **information security** – which itself aims to protect information that can be stored on paper, in computers or even kept by people. Cybersecurity is mainly about protecting electronically stored information and its processing. It is defined as a state in which the risks associated with using information technology, taking into account any threats and vulnerabilities, are reduced to an acceptable level by appropriate measures. The human element, including national interests, also plays an increasingly important role in cybersecurity. So, cybersecurity involves the use of appropriate measures to protect confidentiality, integrity and the availability of information and information technology.

2. SCOPE

This Guide was written for and is applicable to SMEs that rely on technological assets. Its guidelines can be easily implemented by other organisations, whatever their size or complexity.

On the basis of ISO/IEC 27001 content, this Guide describes a series of practical activities that can significantly help with establishing or raising information security levels within an SME. This will strengthen their business and facilitate partnership opportunities within local and EU markets.

All the listed activities ensure an information security lifecycle within the organisation. This includes establishing, planning, implementing, operating and improving all related processes, based on risk culture and continual improvement.

3. INFORMATION SECURITY MANAGEMENT IN AN SME

3.1 STEP 1: ESTABLISH INFORMATION SECURITY FOUNDATIONS

Information security management shares many similarities with other strategic initiatives that organisations may undertake. Before launching any activity, it is essential to define its scope, timeline, and the level of staff involvement. From the outset, top management and a subject-matter expert should be engaged to establish the foundations for the next activities.

The first step requires clear accountability from top management, who must make sure that the organisation's information security direction and objectives are defined. The information security manager holds operational responsibility, while system and information owners should be regularly informed of the progress of tasks. Below, we provide a detailed explanation of the roles that, within an SME, could be assigned to support the secure management of information.

3.1.1 STEP 1.1 ASSIGN ROLES AND RESPONSIBILITIES

In every business and for every activity, it is essential to have properly assigned roles and responsibilities in place. Start-ups or small organisations often view information security as a self-standing process, and one that does not depend on their involvement. Some tend to ignore it completely.

When deciding to take measures to define or revise information security management within an organisation, it is important to define and formalise roles and responsibilities before progressing any further. All subsequent steps have ‘Typically involved roles’ with their RACI:

R = Responsible

A = Accountable

C = Consulted

I = Informed

Main roles and related responsibilities for information security management are generally described in this paragraph. Note that smaller organisations could give more than one role to the same person or outsource these roles (with the sole exception of top management). As a prerequisite step for applying this Guide, every organisation must specifically and formally assign information security roles and responsibilities according to its own structure and culture.

Top management

Ultimate responsibility for information security governance lies with top management, which is part of the overall governance. The main task for top management is to ensure that information security supports the achievement of business goals by demonstrating alignment with an organisation's value delivery, proper resource management and corresponding performance measurements. Top management does not have to be aware of each and every asset within the organisation but is expected to have an overall understanding of critical assets and their value to business operations.

Top management typically includes the Chief Executive Officer (CEO), Chief Operating Officer (COO) or board of directors, depending on the organisation's structure. For the purposes of this Guide, it should be decided who must take on these roles.

PERSONNEL ASSIGNED TO THE DIFFERENT ROLES FOR INFORMATION SECURITY THAT ARE RELEVANT IN THE ORGANISATION SHOULD WRITE DOWN AND ACKNOWLEDGE THEIR RESPONSIBILITIES AND TASKS.

A RACI matrix might help to clarify the assignment of responsibilities and could include the following:

- Determination of information security requirements and classification;
- Risk assessment performance;
- Definition, implementation and maintenance of security measures;
- Acceptance of residual risk;
- System security documentation (norms, procedures, etc.);
- Security policy drafting and update;
- System security monitoring;
- Security improvement plans;
- Awareness and training plans;
- Business continuity plans

For each of these tasks, the following responsibilities should be assigned to the identified roles:

- **Responsible** (referred to as 'R') to carry out the task. There should be at least one person responsible for each task (who might delegate it for assistance);
- **Accountable** (referred to as 'A') to approve the correct completion of the task;
- **Consulted** (referred to as 'C'), whose opinion may be required to develop the tasks, in a two-way communication: they are typically considered to be experts;
- **Informed** (referred to as 'I'), who are kept up-to-date on progress of task development in just a one-way communication.

Information security steering committee

In some cases, SMEs may establish an information security steering committee made up of stakeholders from all the organisation's main departments. It is good practice to have a committee charter, which mainly serves as a tool to achieve consensus amongst major decision-makers. The information security steering committee can work together with top management and will be responsible for auditing and monitoring activities.

When setting up an information security steering committee, it is a good idea to involve the organisation's first lines of reporting to top management and to schedule meetings on a quarterly basis. The committee should meet to deal with several issues related to information security, such as:

- security norms and procedures approval;
- risk analysis review and risk treatment plan;
- audit results and related actions;
- information security plan monitoring;
- information security goal and performance indicators;
- awareness and training sessions planning;
- emergency response.

Information security officer/manager

Even if information security concerns every department in the organisation, it is increasingly common to have an information security manager coordinating relevant activities. This role could be held by any high-ranking staff member (e.g. IT manager or Chief Technology Officer) with good knowledge of information flows.

Since information security is rarely a general management discipline, the information security manager typically instructs top management on major related aspects, prior to acceptance of an information security strategy. Getting top management's commitment is a vital part of information security. One key activity for this is aligning business and information security objectives. Other responsibilities often include: identifying budgets, utilising risk/benefit models for risk estimation and treatment, drafting information security policies and procedures, and reviewing the results of monitoring activities.

The information security manager is also usually responsible for promoting information security awareness, with other possible responsibilities including the establishment of communication channels and reporting. The success of information security depends greatly on communication, both internal and external.

The information security officer/manager is a pivotal figure when applying this Guide: they should be selected for their competences and experience in the field. Their profile, if dedicated for this role, could range from that of security manager to that of a Chief Information Security Officer (CISO). More details on professional profiles and related competences can be found in CWA 16458 on European ICT Professional Profiles.

BENEFITS OF SETTING UP AN INFORMATION STEERING COMMITTEE

WHEN SETTING UP AN INFORMATION SECURITY STEERING COMMITTEE, THE FOLLOWING SHOULD BE CONSIDERED:

- Each department should be represented by the appropriate decision-making authority, to avoid imbalances among different departments, if some areas are not represented by their top managers
- The meeting agenda should be planned and distributed in advance
- The meetings should be held periodically (i.e.every three months) and systematically
- Meeting rules should be established, including any decisions on who leads the meeting and how to solve potential conflicts
- Relevant information security decisions should be made in this committee
- Time schedules should be respected

System and information owners

More structured organisations might need to identify a series of individuals to carry out tasks on a daily basis, in order to protect the information systems that they control. These are the 'system owners'. However, business owners in charge of processes and data should be involved in defining the requirements for their protection, regardless of information systems. These are the 'information owners'. Both categories should help the organisation by ensuring that information security controls are in place and are performing adequately.

Usually the owners have the right to make changes to whatever they own, e.g. system improvements, create shortcuts, etc. However, these decisions should always take into account information security impacts. For this model to work, it must be made clear who the system and information owners within the organisation are. This begins with a minimal approach by the IT manager and the Chief Operating Officer (COO), with both involved. Moreover, the organisation may often struggle to find system and information owners at the lower levels of management hierarchy – people who decide on asset enhancement or shortcuts. Doing this requires the delegation of decision-making practices and a consistent culture.

Personnel

The success of information security depends on proper training and education for personnel. Employees and contractors should fully understand the reasons behind the control environment surrounding them, so they can maintain information security at the right level and not compromise it.

Employees and contractors should be able to recognise unusual behaviour and quickly raise any concerns to the information security manager, in order to minimise loss for the organisation. Quite often employees and contractors are the targets of attacks. So having educated staff considerably enhances the overall information security environment. These staff may also be able to turn that knowledge and expertise into organisational culture.

3.2 STEP 2: UNDERSTAND WHAT MUST BE PROTECTED

From this chapter on, this Guide will complement the description of each of the tasks suggested for the safe management of information within an organisation with examples (e.g. figures, tables, etc.). These examples will help the reader to understand the Guide.

Before applying any information security measure, an organisation needs to get an initial clear view of which objects really have value for it. Such objects, usually defined as assets, can be

generally classified under information (see Step 2.1), which are typically intangible, and other assets (see Step 2.2), which are typically tangible.

The main objective of this action is to represent the key assets that are under the control of the organisation and need protection. This is especially important when identifying relations between assets and when defining responsibilities.

Typically involved roles: top management (A), information owners (C), system owners (C), information security manager/officer (R).

3.2.1 STEP 2.1 IDENTIFY WHAT INFORMATION IS USED

It is useful to build an asset map, starting from intangible assets: the organisation's information.

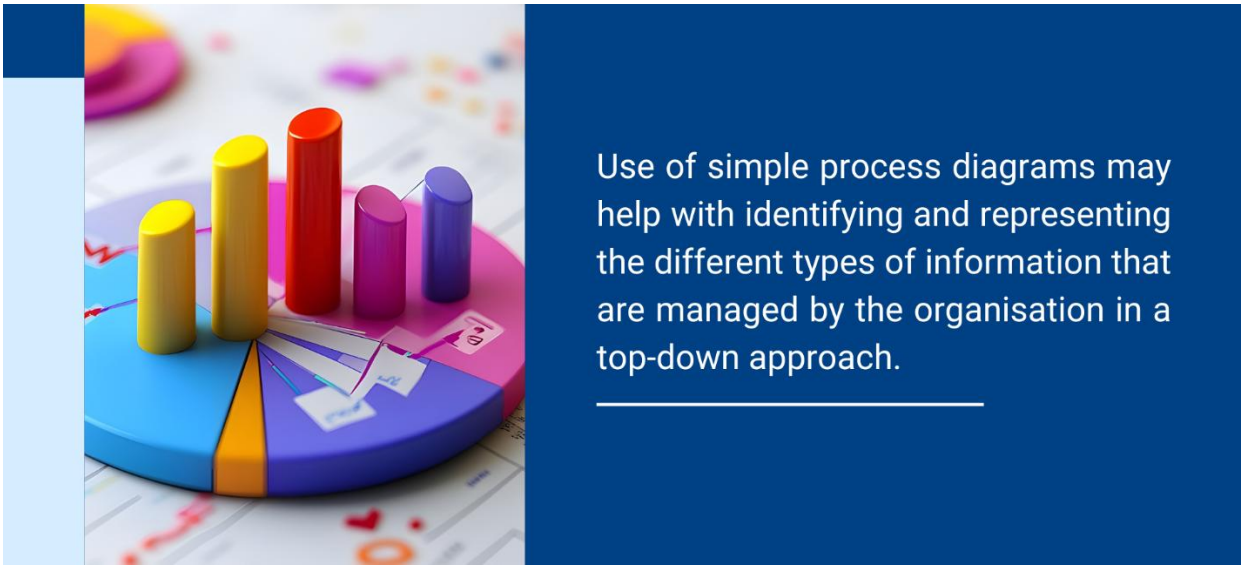
Top-down approach

An organisation might choose to adopt a 'top-down' approach, in which information (the white boxes below) are identified as they flow among processes (the coloured boxes below).

Figure 1: Example of asset map with reference to hypothetical information within a given organisation

For the best use of a top-down approach, the organisation should have a good understanding of its processes, e.g. be aware of their nature, know who is responsible for each process, etc. The link between the organisation's activities and information can be made clear by starting with a bird's eye view of processes and drilling down to information assets. Information owners (usually business or department managers) are the most appropriate people to classify and evaluate the relevance of such information inside the organisation. It is a good idea to conduct a short

interview with each information owner, in order to get a comprehensive view of the information managed by the organisation.



Bottom-up approach

The top-down approach requires a good understanding of organisational processes, whereas this is not necessary for a 'bottom-up' approach. The latter can be used by any organisation, regardless of maturity level. When implementing a bottom-up approach, an ideal starting point is to get an answer to the question "What kind of information does the organisation handle overall?" This question can be put to the person/persons with an overall view of the organisation. Below is a simple list to ensure that everything important is considered:

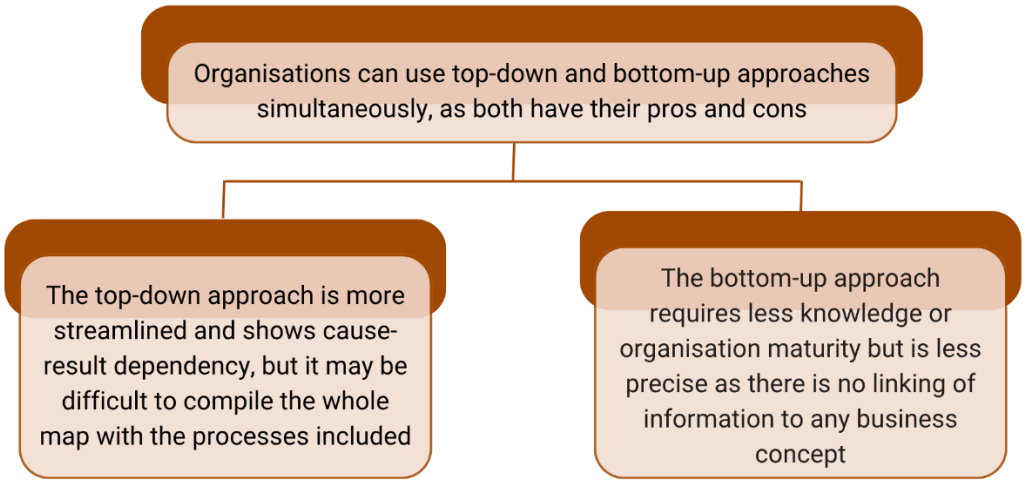
a) personal data (e.g. name, addresses, SSNs, payrolls);

b) sensitive personal data (e.g. healthcare diagnoses, political beliefs, payment card data);

c) strategic enterprise data (e.g. business plans, forecasts, pre-release budget statements);

d) project/design data (e.g. product design, proprietary source code);

e) other enterprise data (e.g. monitoring data, production statistics, tax facts).



After building an asset map, the organisation should have a good understanding of its information assets at a conceptual level, regardless of which storage or processing equipment is used.

3.2.2 STEP 2.2 IDENTIFY WHICH OTHER ASSETS ARE USED

Identified information can be stored, processed or transmitted using several other assets, mostly (but not exclusively) technological. Those assets are usually layers of software which run on information systems but can also be paper files and disks or services provided by external service providers. A bottom-up approach is usually needed to correctly identify them, i.e. involving IT personnel and application administrators (whether or not they are formally designated as system owners). It is highly recommended that key assets, which belong at least to the following asset categories, are not overlooked:

1) endpoints (laptops, desktops, tablets, smartphones), servers and appliances;
2) end-user software (not including office automation suites or operating systems);
3) service providers (including workforce, housing/hosting and cloud providers);
4) personnel (direct employees and subcontracted employees);
5) physical locations (directly owned offices and computer rooms).

Those elements can also be investigated initially during a top-down interaction with information owners as described in the previous step, just after defining information related to processes and

then refined with the system owners. Building on the example above, we could end up with a structured list like this:

Software	Hardware	Personnel	Providers	Locations
CRM application ERP application Shared folders	Production servers Testing servers Staff PCs Staff smartphones	Internal staff	Cloud provider TLC provider	Main offices

Figure 2: Example of asset map identifying key assets other than information within a given organisation

3.2.3 STEP 2.3 UNDERSTAND THE CONNECTION BETWEEN INFORMATION AND OTHER ASSETS

Once all key assets are identified, establishing which ones are used for certain information is a simple but effective way to understand what needs protection and, later on, how much protection it needs. In order to do this, a simple matrix can be created, like the one below. Here filled cells show a connection between assets and information; blank cells show that there is no connection.

	General customer data	Customer claims	Source code	Design specifications	Requests for proposals
CRM application	X	X			
Production servers	X	X			X
Testing servers			X		
Staff PCs	X	X	X	X	X
Staff smartphones	X	X			
Shared folders				X	
ERP application					X
Internal staff	X	X	X	X	X
Cloud provider	X	X			X
TLC provider	X	X			X
Main offices	X	X	X	X	X

Table 1: Example of matrix for identifying the connection between information and other assets

With those relationships clearly established, the asset map is completed. This will be of great help in the following steps. Of course, more information can be gathered for each asset, up to a complete asset inventory that can used to better manage them all. Remember that the asset map must be constantly updated, otherwise it will quickly become less useful.

3.3 STEP 3: EVALUATE INFORMATION SECURITY RISKS

Information security risk assessment is focused on finding out beforehand what can possibly go wrong with the assets and have a negative impact on the cash flow, legal obligations or reputation of a given organisation. This step is crucial for understanding the threats that the organisation is facing, so that appropriate controls can be implemented to avoid, contain or ensure recovery from their occurrence. By prioritising risks, each organisation can concentrate defensive resources where the biggest losses are most likely to be caused, thus ultimately optimising the effectiveness of these resources.

Typically involved roles: top management/information security steering committee (A), information owners (C), system owners (C), information security manager/officer.

3.3.1 STEP 3.1 UNDERSTAND THE VALUE OF ASSETS

To make the asset map (see Step 2.3) fully fit for the risk assessment process, one key element should be added: an evaluation of the importance of each asset within the organisation.

The simplest way to do this evaluation is to start from the defined information and to consider at least two of the main security-related properties on information: **availability and confidentiality**. Integrity can be added, but in the simplest contexts it can be considered as closely related to availability. A basic evaluation of information defined in Step 2.1 should be made, with each information owner using the following table as a reference, assigning a value to availability and confidentiality to each identified item of information.

	Low Value	High Value
Availability (Av.)	Could the unavailability of this information significantly impact the organisation's business activities or reputation?	
	No	**Yes**
Confidentiality (Conf.)	Could the unauthorised dissemination of this information cause relevant competitive damage to the organisation or violate major laws/contract obligations?	
	No	**Yes**

Table 2: Evaluation of assets for their availability and confidentiality

Applying the table above to the example could result in the following values:

General customer data	Customer claims	Source code	Design specifications	Requests for proposals	Purchase orders
Av: low Conf: high	Av: low Conf: low	Av: low Conf: high	Av: low Conf: high	Av: high Conf: low	Av: low Conf: high

Table 3: Example of evaluation of information for its availability and confidentiality

Since all other assets have their main values related to the information they store, process or transmit, this first evaluation can be inherited by all assets connected with the evaluated information in the asset map. This assumes that their relationship with the highest evaluated information gives them their true value for the organisation, as shown below.

	General customer data	Customer claims	Source code	Design specs	Requests for proposals	
	Av: low Conf: high	Av: low Conf: low	Av: low Conf: high	Av: low Conf: high	Av: high Conf: low	
CRM application	X	X				Av: low, Conf: high
Production servers	X	X			X	Av: high, Conf: high
Testing servers			X			Av: low, Conf: high
Staff PCs	X	X	X	X	X	Av: high, Conf: high
Staff smartphones	X	X				Av: low, Conf: high
Shared folders				X		Av: low, Conf: high
ERP application					X	Av: high, Conf: low
Internal staff	X	X	X	X	X	Av: high, Conf: high
Cloud provider	X	X			X	Av: high, Conf: high
TLC provider	X	X			X	Av: high, Conf: high
Main offices	X	X	X	X	X	Av: high, Conf: high

Table 4: Example of matrix for comprehensively identifying the connection between assets and their evaluation for availability and confidentiality

This completed and enhanced asset map, however it is represented, provides a good answer to the question of what needs information security protection and how much of it, depending on the asset's effective role.

To evaluate the assets, different scales may be used (e.g. a low/medium/high evaluation can be performed). To enhance such an analysis, the impact may be evaluated taking into consideration additional criteria, such as:

- **Legal requirements**
- **Economic or commercial interests**
- **Reputation (public image)**
- **Safety**

3.3.2 STEP 3.2 EVALUATE THE TYPE OF CONTEXT IN WHICH THE ORGANISATION WORKS

A thorough understanding of the environment in which the organisation operates is of key importance when defining information security requirements. ENISA, the EU Agency for Network and Information Security, has developed a cybersecurity threat model: this is useful when considering all the likely threats facing the organisation. ENISA's model has the following threat categories:

a) Disaster (e.g. earthquake, flood, fire);

b) Outage (e.g. strike, essential service unavailability);

c) Physical attack (e.g. theft, sabotage);

d) Legal (e.g. breach of regulation, court order);

e) Unintentional damage (e.g. information leak, loss of a device);

f) Failures-malfunction (e.g. hardware failure or malfunction);

g) Nefarious-activity-abuse (e.g. malware, social engineering, brute force);

h) Eavesdropping-interception-hijacking (e.g. espionage, man in the middle).

The applicability of those threats should be evaluated, by considering historical incident data (where available) and staff experience. An evaluation like this could at least establish how for example the following conditions apply to the organisation's environment:

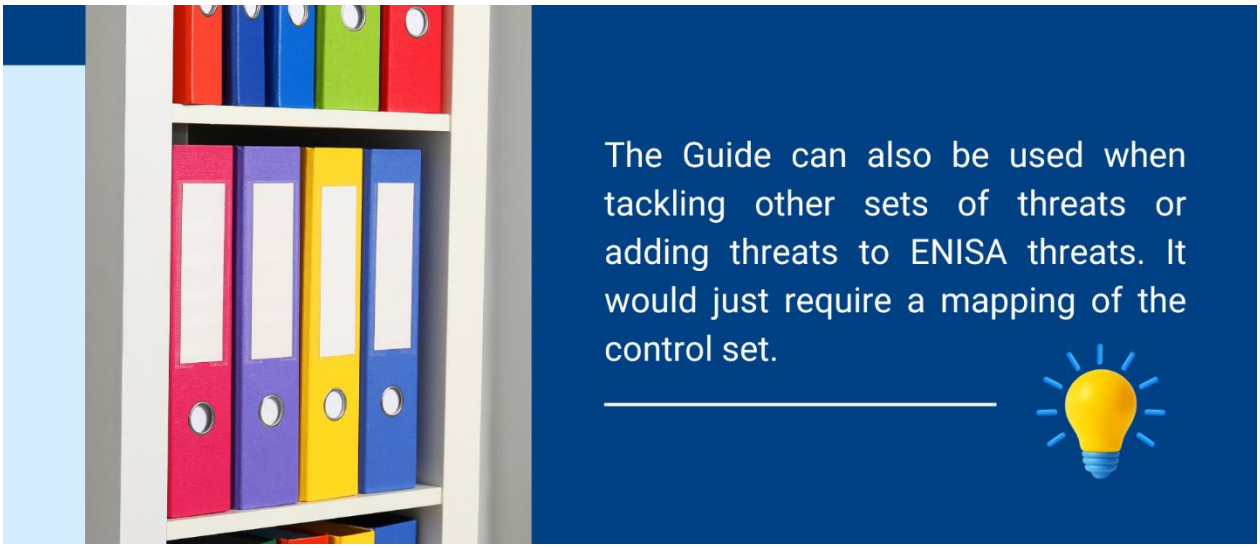
1) How prone are the organisation's premises to natural disasters or incidents (floods, fires, earthquakes)?
2) How prone are the organisation's premises to service outages (Internet connections, power loss, strikes)?
3) How faithful is the personnel (small turnover, no unrest, team cohesion)?
4) How strongly do regulations or contractual requirements impact the business?
5) How prone is the organisation to the personnel's human errors?
6) How dependent is the business on external providers?
7) To what extent do ICT services expose the organisation to the Internet?
8) How important is the organisation's public reputation?

THE RELEVANT INFORMATION AND ASSET OWNERS FOR ANSWERING THOSE QUESTIONS MIGHT BE:

- **IT MANAGER** for unintentional damage, disaster, failures/malfunction, outages, eavesdropping-interception-hijacking, nefarious-activity-abuse threat categories;
- **SECURITY / FACILITY MANAGER** for physical attack, disaster, failures/malfunction threat categories;
- **LEGAL MANAGER** for legal threat category;
- **HUMAN RESOURCES MANAGER** for outages threat category.

The answers to those questions (which can result in High/Low/None values), obtained by consulting the relevant information and asset owners, can really help when determining the likely threats that the organisation will face, directly relating (1 to a, 2 to b, etc.) to the ENISA

cybersecurity threat model. Those considerations should be separate from the organisation's in-place measures.



All threats for which the corresponding questions have been valued differently from 'None', and which are applicable to any of the identified assets as described by the following table, must be considered as potential risk causes for the organisation.

	Disaster	Outages	Physical attack	Legal	Unintentional damage	Failures-malfunction	Nefarious-activity-abuse	Eavesdropping-interception-hijacking
Hardware	X		X		X	X	X	
Software				X	X	X	X	X
Service providers		X		X		X		X
Personnel	X	X		X			X	X

Physical locations	X		X					

Table 5: Example of matrix to be used for evaluating the type of context in which the organisation works

For instance, if the answer to question 3) was 'Low', the corresponding threat c) related physical attack would apply to hardware and physical location assets. In the example asset map (Figure 2), this would be production servers, testing servers, staff PCs, staff smartphones and main offices.

3.3.3 STEP 3.3 IDENTIFY WHICH CONTROLS ARE ALREADY IN PLACE

Information security controls are the core elements in charge of reducing risks: they can do this significantly if well implemented. Several controls are often already present, but they are numerous and should be considered not just at an organisation's level but, in most cases, also at an asset level in order to identify any protection shortcomings.

ISO/IEC 27001 Annex A is a remarkable list of controls, intentionally created to allow an organisation to make a 'completeness' check of potentially applicable controls. This list has been simplified for application to SMEs in the Annex A of this Guide, while keeping track of the reference to original ISO/IEC 27001 Annex A controls. Each control in the list should be marked if it is already fully applied or not (partial application will be conservatively considered as non-applications) for each group of assets related to an item of information.

3.4 STEP 4: DESIGN, APPLY AND MONITOR INFORMATION SECURITY CONTROLS

As soon as the organisation is fully aware of what should be protected and how it is currently protected, decisions can be taken about the controls to be newly implemented or improved. The top management/information security steering committee should evaluate what must be done in order to address each particular risk, along with timing and funding for each solution. Most

proposals usually come from the information security manager/officer. The selected protective measures should be effective and cost-efficient.

Typically involved roles: top management/information security steering committee (A), information owners (R), system owners (R), personnel (R), information security manager/officer (R).

3.4.1 STEP 4.1 IDENTIFY CONTROLS TO BE IMPLEMENTED AND SET UP AN INFORMATION SECURITY PLAN

Deciding which controls are to be implemented in a specific environment is the toughest decision in the whole information security field. No combination of controls is perfect for every situation, because this could result in higher-than-necessary costs, as well as creating lots of controls, and incidents that are not so easy to predict, and so on.

In line with the previous steps and according to relevant good practices, this Guide proposes in its Annex A the classification of controls into two main categories:

1) baseline controls, ideally to be implemented in every situation;

2) discretionary controls, which should be used to protect assets of high value, subject to likely threats.

Baseline controls are grouped in the first section of Annex A (A.1) and, unless specific situations arise, they should always be implemented. Annex X of this Guide is proposed as an ideal example of the baseline control: the information security policy. Once completed, this policy document should be formally approved by the organisation's top management in order to correctly identify priority and resources within the organisation's context.

Discretionary controls are grouped in the second section of Annex A (A.2). Here, each control is associated with the threats that it mitigates in the third section of Annex A (A.3). If no value is present in the corresponding threat cell in the A.3 section, the control does not mitigate it significantly. If the 'Secondary' value is present, this means it does so sensibly. Finally, if the 'Primary' value is present, this means it does so more effectively. Since every asset has been given a value in Step 3.1 and has been associated with applicable threats in Step 3.2, those elements can simply help users to decide whether or not to apply a control. If an asset has a high confidentiality or availability value OR is a highly likely threat, then only controls marked as 'Primary' for that specific threat should apply. If an asset has both a high confidentiality or

availability value AND is a highly likely threat, then it is worthwhile also considering controls marked as 'Secondary' for that specific threat.

For instance, staff smartphones – whose evaluation in table 4 is 'Av:low, Conf:high' – are hardware, and so they are subject to a 'Low' physical attack threat. All controls which have a 'Primary' relationship with the physical attack threat would need to be applied to staff smartphones as well as to baseline controls. This means:

- A2.06 Removable media management;
- A2.10 Physical security;
- A2.11 Environmental threats protection;
- A2.12 Equipment maintenance;
- A.2.16 Backup.

This Guide can also be used when tackling other sources of controls rather than those presented in Annex A or when adding other controls to it. In this case, the threat set must be re-mapped.

A check of the applied controls detected in the previous step, and the ones resulting from the three abovementioned categories, should be performed at an asset level. Where the current situation results in a control that is less effective than recommended or is missing, this situation should be noted and further analysed. The list of those controls forms the basis for building an Information Security Plan, which will allow the organisation to selectively improve its information security protection. The Information Security Plan should include more elements than a simple list of

controls. For example, it could include a set of actions with related owners, times, costs and other information. It can effectively be as simple as a spreadsheet with the following fields:

Code	Id
Source	Source activity
Action description	Descriptive text
Owner	Function or person
Cause	Activity motivation
Priority	Low
Status	Open/Closed
% progress	0%-100%
Resource	Costs, personnel
Start date	dd/mm/yy
End date	dd/mm/yy
Notes	Other annotations

Table 6: Template for the tracking of actions to be implemented under an Information Security Plan

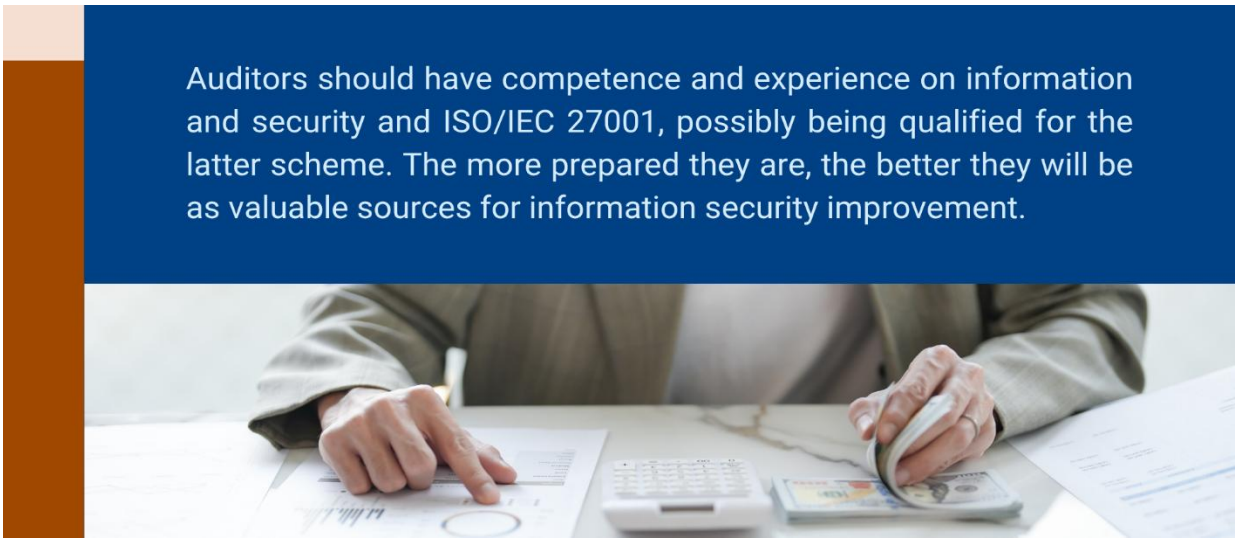
3.4.2 STEP 4.2 MANAGE THE INFORMATION SECURITY PLAN

Once approved, the information security manager/officer should be responsible for periodic (e.g. monthly or quarterly) monitoring, in order to assess whether the Information Security Plan is progressing well and includes the largest possible involvement of other interested parties. This monitoring should be done through a formal committee (e.g. the information security steering committee) meeting: all the professionals involved should report on their progress, difficulties and changes to be applied to the plan. The plan should be updated accordingly and, if significant changes are applied requiring new resources, it should be submitted again to top management for approval. If no significant changes are applied, the plan should still be reapproved by top management periodically (at least every year, possibly before the next year's budgets are finalised in order to allow the correct allocation of resources).

The plan should also include the results of new actions suggested or otherwise mandated by the activities performed in the following *Step 4.3*.

3.4.3 STEP 4.3 CONTROL INFORMATION SECURITY

An effective way to verify whether the information security is being correctly maintained is to plan and do information security audits, which should take place at least annually. Auditors should be selected from among impartial subject-matter experts: they should be tasked with verifying the compliance of information security processes with internal and external requirements. If the audit is done by internal staff, the auditor will not have operational responsibilities in information security management, so as to avoid a conflict of interest.



As a result of the audit, the organisation's top management should receive a report with:

- Non-conformities, i.e. aspects where the organisation is not fulfilling the standard;
- Improvement opportunities, i.e. recommendations to work in a safer way (although the standard is fulfilled).

Non-conformities should be carefully analysed and actions implemented, thus avoiding their recurrence in the future. Such actions must be included in an updated version of the Information Security Plan, along with the actions necessary to correct non- conformities. Improvement opportunities should be evaluated and if necessary inserted within the Information Security Plan too, if deemed relevant, usually with a less strict priority than the actions to address non-conformities.

3.4.4 STEP 4.4 MONITOR INFORMATION SECURITY

After having defined and designed the protections included in the previous step, the organisation can get back to 'business as usual'. To ensure the system's effectiveness, monitoring activities will help to limit deviations from the initial Information Security Plan.

The most practical way to carry our monitoring activities is to build some simple yet effective goal or performance indicators: these can be periodically updated. Indicators like this can be based on objectives or controls: they are essentially made up of formulas to calculate thresholds that should trigger some action when breached or reached. It is important to assign the responsibility for periodically applying the formula to the indicator. The ISO/IEC 27004 standard may help when developing this task.

Goal indicators are the simplest indicators to set up. They can be used to measure the reaching of a relevant objective for the organisation, such as obtaining compliance status with the present guideline or with a relevant regulation/standard, a security- related service level or status. They should be verified every few months.

The use of a red/ amber/ green colour code helps to identify visually whether the indicator is fulfilled, almost fulfilled (considering for example a range of 5%) or not fulfilled at all. For a quick and visual overview of its evolution, the indicator can be depicted in a linear or bar graph.

Performance indicators can be related to some performance values from information security processes (e.g. risk assessment) or to controls effectiveness. In the latter case, the basic controls proposed in Step 3.1 can be associated with indicators like these examples:

Control	Indicator formula	Target	Periodicity
Information security policy	% of the employees that have received the policy	100%	annual
Information security organisation	# of information security steering committee meetings	4	annual
Information security awareness, education and training	% of the employees that have received training, # of security awareness initiatives	100%	annual
Asset inventory	% of assets included in the asset inventory within 1 month of their acquisition	100%	quarterly
Malware protection	# of infected workstation/cleaned workstation	1	monthly
Software vulnerability patching	# of outstanding critical security patches	0	monthly
Security in supplier agreements	% of contracts with specified information security clauses	100%	quarterly
Incident response	# of information security incidents closed / information security incidents open in the same day	95%	monthly

Table 7: Suggested periodicity for the monitoring of controls

These are just some basic examples. Each organisation has to consistently determine its own indicators. These indicators, which may be tracked in a simple spreadsheet, can be periodically examined by the information security officer/manager or presented to the information security steering committee.

Deadlines to be met should be fixed for each target. Other thresholds can vary in time and be set at a lower value than the target initially, increasing with the maturity of the process or control

involved. The information security steering committee can periodically monitor the status and development of information security management.

4. ISO/IEC 27001 CERTIFICATION

The approach suggested so far is closely related to ISO/IEC 27001 requirements, as suggested by the following mapping table. Where there is no correspondence between the international standard and this Guide, this is due to the simplified approach followed by the Guide's authors: this approach aims to remove the most formal and methodological aspects while focusing on the most practical aspects.

ISO/IEC 27001:2013 main chapters		Digital SME Guide steps
4.1	Understanding the organisation context	Step 3
4.2	Understanding the need and expectations of interested parties	Step 2
4.3	Determining the scope of the information security management system	N/A
4.4	Information security management system	N/A
5.1	Leadership and commitment	N/A
5.2	Policy	*Baseline control* A1.01
5.3	Organisational roles' responsibilities and authorities	Step 1
6.1	Actions to address risks and opportunities	Step 2 Step 3
6.2	Information security objectives and plans to achieve them	N/A
7.1	Resources	N/A
7.2	Competence	N/A
7.3	Awareness	*Baseline control* A1.03
7.4	Communication	*Discretionary control* A2.01

7.5	Documented information	N/A
8.1	Operational planning and control	Step 4
8.2	Information security risk assessment	Step 2 Step 3
8.3	Information security risk treatment	Step 4
9.1	Monitoring, measurement, analysis and evaluation	Step 4
9.2	Internal audit	Step 4
9.3	Management review	
10.1	Non-conformity and corrective action	Step 4
10.2	Continual improvement	

Table 8: Main contents of ISO/IEC 27001:2013

Nevertheless, any such (no correspondence) cases would need to be addressed, if a formal certification against ISO/IEC 27001 standard becomes an objective to be pursued after information security management is performed for some time on the basis of this Guide. More specifically, the following additional activities should be executed after Step 1.1, as presented in chapter 3.

4.1.1 STEP 4.1 ESTABLISH THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

An Information Security Management System (ISMS) should be considered a more formal approach towards information security management than the approach described in this Guide. An ISMS will comprise policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information. Top management should be directly involved in planning an ISMS, which introduces more formalities but also enables progress towards an internationally recognised certification for a part of the organisation. Care should be taken when selecting this part, because its extension would directly impact on the certification costs. Selecting the entire organisation is feasible but not the only

choice, since key services or processes could be prioritised in line with the organisation's business strategies. Note that it is also feasible to certify just one part of a more widely established ISMS.

Early top management involvement would be essential when shaping the scope, as well as for gaining additional key commitment (and then resources) to be used in the following steps. Implementation progress should be regularly reported on, with deadlines set for this implementation.

Measurable and business-related objectives should be proposed and selected in this phase. Those objectives, like all the rest of the ISMS, should always be focused on continuous improvement, iteration after iteration.

4.1.2 OTHER ELEMENTS

The document management approach, to be followed under a formal ISMS (and for every management system), also requires that every produced document:

- features complete metadata (title, date, author as a minimum);
- is built upon established formats and models;
- is under control of changes/versions;
- is distributed to its intended audience.

A statement of applicability document pursuant to ISO/IEC 27001 requirement 6.1.3 d) should be produced and kept up-to-date. The proposed template for control selection in this Guide is a good starting point, but it must at least include justification for any inclusion or exclusion of each control.

A formal management review, which includes all input elements specified in ISO/IEC 27001 requirement 9.3, should also be periodically performed. It should use the same approach suggested in Step 3.2, but it should also be put into words.

The formal third-party certification activity may also be added. This can be done in the same way as an internal audit, whilst leveraging an external and competent view on the ISMS.

5. REFERENCES AND FREELY ACCESSIBLE RESOURCES

REFERENCES

- ISO/IEC 27000 family – Information security management systems. Available online at: https://www.iso.org/isoiec-27001-information-security.html

FREELY ACCESSIBLE RESOURCES

- BSI. ISO/IEC 27001 for small and medium-sized businesses (SMEs). Available online at: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISO- 27001-for-SMEs/
- Centre for Cyber Security Belgium. Cyber Security Guide for SMEs. Available online at: https://cybersecuritycoalition.be/resource/cyber-security-guide-sme/
- ETSI. Implementation of the Revised Networks and Information Security (NIS2) Directive applying Critical Security Controls – ETSI TS 103 992 – technical report released by ETSI's technical committee on Cybersecurity (TC CYBER). Available online at: https://www.etsi.org/deliver/etsi_ts/103900_103999/103992/01.01.01_60/ts_103992v010101p.pdf
- ISO. Publicly available standards (including ISO/IEC 27000). Available online at: https://www.iso.org/sectors/security-safety-risk
- ENISA. Risk Management Standards. Available online at: https://www.enisa.europa.eu/sites/default/files/publications/O.7.2-T2-Risk_Management_standards.pdf
- ENISA. Cybersecurity for SMEs – Challenges and Recommendations. Available online at: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
- ENISA. Cybersecurity guide for SMEs – 12 steps to securing your business. Available online at: https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

ANNEX A

A.1 Baseline controls

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
01	Policies for information security	5.1	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and revised at planned intervals and if significant changes occur. Suggested review frequency: annual
02	Information security roles and responsibilities Segregation of Duties	5.2 5.3	Information security roles and responsibilities shall be defined and allocated according to the organisation needs. Conflicting duties and conflicting areas of responsibility shall be segregated. Suggested review frequency: annual
03	Information security awareness, education and training	6.3	Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function. Suggested training frequency: annual
04	Inventory of Assets Acceptable Use of Assets Return of Assets Classification of Information	5.9 5.10 5.11 5.12	An inventory of information and other associated assets, including owners, shall be developed and maintained. Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented. Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their emplyment, contract or agreement. Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability, and relevant interested party requirements.

			Suggested review frequency: monthly
05	Classification of Information Labelling of Information Handling of Information	5.12 5.13 5.14	Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability and relevant interested party requirements. An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organisation. Information transfer rules, procedures, or agreements shall be in plance for all types of transfer facilities within the organisation and between the organisation and other parties. Suggested review frequency: Annual
06	Identity Management Authentication Information	5.16 5.17	The full life cycle of identities shall be managed. Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. Suggested review frequency: When organisational change occurs
07	Access Rights Priviliged Access Rights	5.18 8.2	Access rights to information and other associated assets shall be provisioned, reviewd, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control. The allocation and use of privileged access rights shall be restricted and managed. Suggested review frequency: When organisational change occurs
08	Authentication Information	5.17	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information. Suggested review frequency: When organisational change occurs
09	Physical security monitoring Protecting against physical and environmental threats	7.4 7.5 7.7	Premises shall be continuously monitored for unauthorised physical access. Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.

	Clear desk and clear screen		Suggested review frequency: Monthly
10	Protection against malware	8.7	Protection against malware shall be implemented and supported by appropriate user awareness. Suggested review frequency: Monthly
11	Management responsibilities	5.4	Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation. Suggested review frequency: Monthly
12	Management of technical vulnerabilities	8.8	Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken. Suggested review frequency: Monthly
13	Networks Security Security of network services	8.20 8.21	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications. Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored. Suggested review frequency: Monthly
14	Information Security in Supplier Relationships Addressing information security within supplier agreements	5.19 5.20	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services. Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship. Suggested review frequency: Annual
15	Information security incident management planning and preparation Assessment and decision on information	5.24 5.25 5.26 5.27	The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities. The organisation shall assess information security events and decide if they are to be categorised as information security incidents. Information security incidents shall be responded to in accordance with the documented procedures.

	security events Response to information security incidents Learning from information security incidents		Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls. Suggested review frequency: When organisational change occurs
16	Legal, statutory, regulatory and contractual requirements Intellectual property rights	5.31 5.32	Legal, statutory, regulatory and contractual requirements relevant to information security and the organisation's approach to meet these requirements shall be identified, documented and kept up to date. The organisation shall implement appropriate procedures to protect intellectual property rights. Suggested review frequency: Annual

A.2 Discretionary controls

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
01	Contact with authorities Contact with special interest groups	5.5 5.6	The organisation shall establish and maintain contact with relevant authorities. The organisation shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.
02	Remote working	6.7	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.
03	Inventory of information and other associated assets Acceptable use of information and other associated assets Return of assets	5.9 5.10 5.11	An inventory of information and other associated assets, including owners, shall be developed and maintained. Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented. Personnel and other interested parties as appropriate shall return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.
04	Screening	6.1	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations, and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risk.
05	Terms and conditions of employment Information security	6.2 6.3	The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security. Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-

	awareness, education and training		specific policies and procedures, as relevant for their job function.
06	Storage media	7.1	Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.
07	Secure disposal or re-use of equipment	7.14	Items of equipment containing storage media shall be verified to ensure to any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.
08	Access control	5.15	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements
09	Use of cryptography	8.24	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.
10	Physical security perimeters Physical entry Securing offices, rooms and facilities Physical security monitoring	7.1 7.2 7.3 7.4	Security perimeters shall be defined and used to protect areas that contain information and other associated assets. Secure areas shall be protected by appropriate entry controls and access points. Physical security for offices, rooms and facilities shall be designed and implemented. Premises shall be continuously monitored for unauthorised physical access.
11	Protecting against physical and environmental threats	7.5	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.

12	Equipment maintenance	7.13	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.
13	Clear desk and clear screen	7.7	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.
14	Change management	8.32	Changes to information processing facilities and information systems shall be subject to change management procedures.
15	Separation of development, test and production environments	8.31	Development, testing and production environments shall be separated and secured.
16	Information backup	8.13	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.
17	Logging Monitoring activities	8.15 8.16	Logs that record activities, exceptions, faults and other relevant events shall be produces, stored, protected and analysied. Networks, systems and applications shall be monitored for anomalous behaviours and appropriate actions taken to evaluate potential information security incidents.
18	Clock synchronisation	8.17	The clocks of information processing systems used by the organisation shall be synchronised to approved time sources.
19	Segregation of networks	8.22	Groups of information services, users and information systems shall be segregated in the organisation's network.

20	Information transfer	5.14	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.
21	Secure system architecture and engineering principles	8.27	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.
22	Application security requirements	8.26	Information security requirements shall be identified, specified and approved when developing or acquiring applications.
23	Secure development life cycle	8.25	Rules for the secure development of software and systems shall be established and applied.
24	Security testing in development and acceptance	8.29	Security testing processes shall be defined and implemented in the development life cycle.
25	Monitoring, review and change management of supplier services	5.22	The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.
26	Information security incident management planning and preparation	5.24	The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.
27	Learning from information security incidents	5.27	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls

28	Redundancy of information processing facilities	8.14	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements
29	Intellectual property rights	5.32	The organisation shall implement appropriate procedures to protect intellectual property rights.
30	Independent review of information security Compliance with policies, rules and standards for information security	5.35 5.36	The organisation's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur. Compliance with the organisation's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.

A.3 Discretionary controls threat relationship (mitigation)

Control	ISO/IEC 27001	Physical attack	Unintentional damage	Disaster	Failures-malfunction	Outages	Eavesdropping-interception-hijacking	Legal	Nefarious-activity-abuse
Contact with authorities **Contact with special interest groups**	5.5 5.6	Secondary		Primary			Primary	Primary	Secondary
Remote working	6.7	Secondary	Secondary		Secondary	Primary	Primary		Primary
Inventory of information and other associated assets	5.9 5.10 5.11	Secondary	Primary	Secondary	Secondary	Secondary	Primary	Secondary	Primary
Acceptable use of information and other associated assets	6.1	Secondary						Primary	Primary
Return of assets	6.2 6.3						Secondary	Primary	Primary
Screening	7.1	Secondary		Secondary	Primary	Secondary	Primary		Secondary
Terms and conditions of employment	7.14	Secondary		Primary	Secondary	Secondary	Primary		Secondary
Information security awareness, education and training	5.15	Primary		Secondary			Primary	Secondary	Primary
Storage media	8.24						Primary		Primary

Secure disposal or re-use of equipment	7.1 7.2 7.3 7.4	Primary	Secondary	Primary			Secondary	Secondary	Primary
Access control	7.5	Primary	Secondary	Primary	Secondary	Primary			
Use of cryptography	7.13	Secondary	Primary	Secondary	Primary	Primary			
Physical security perimeters	7.7	Secondary	Secondary	Secondary			Primary		Secondary
Physical entry	8.32				Primary	Secondary	Secondary	Secondary	Primary
Securing offices, rooms and facilities	8.31				Secondary	Secondary	Secondary		Primary
Physical security monitoring	8.13			Primary	Secondary	Primary	Secondary		
Protecting against physical and environmental threats	8.15 8.16						Primary	Primary	Primary
Equipment maintenance	8.17					Primary			Secondary
Clear desk and clear screen	8.22						Primary		Primary
Change management	5.14						Primary	Primary	Secondary
Separation of development, test and production environments	8.27						Secondary	Primary	Primary
Information	8.26						Secondary	Primary	Primary

backup									
Logging	8.25						Secondary	Primary	Primary
Monitoring activities	8.29						Secondary	Primary	Primary
Clock synchronisation	5.22				Primary	Primary	Secondary	Primary	Primary
Segregation of networks	5.24			Primary	Primary	Primary	Secondary	Primary	Primary
Information transfer	5.27							Primary	Primary
Secure system architecture and engineering principles	8.14			Primary	Primary	Primary			
Application security requirements	5.32						Primary	Primary	Primary
Secure development life cycle	5.35 5.36							Primary	Primary

ANNEX X

Information Security Policy		
Policy #:	**Effective Date:**	**Email:**
Version:	**Contact:**	**Phone:**

Purpose

The information security policy, related policies and procedures of the company are intended to protect the confidentiality, integrity and availability (CIA) of all the organisation's critical data and assets according to its business interests.

Scope

This policy applies to employees, contractors, consultants, temporary workers, and other workers at the organisation, including all personnel affiliated with third parties. This policy applies to all assets, both tangible and intangible, owned or used by the organisation.

Policy

The organisation's top management considers information security among the key enabling factors for its business and is actively committed to promote and fund all initiatives that would cost-effectively reduce information security risks, ensure compliance to relevant laws and contractual requirements, and follow the sectoral good practices. All the organisation's internal and external personnel are expected to diligently follow the intent and prescriptions of the present policy and of all related policies and procedures. They can face disciplinary action for not doing so. More specifically, the information security principles that everyone is expected to understand and observe are:

1) Information security is not absolute; it must always be proportionate to the risks it must counter.

2) All access must be strictly bound to the need to know about the personnel and about their job needs.

3) Resources should be split and protected according to their information security requirements.

4) Using open standards and solutions is always preferable to proprietary and obscure choices.

5) A single layer of information security controls may not be sufficient in all cases since it can fail multiple layers approaches may be used where a failure would be critical.

6) Studying, exercising and testing information security relevant situations is the key to ensuring effective response readiness.

7) Information security is everybody's responsibility and duty; it is not someone else's problem.

The organisation defines and measures a set of specific information security objectives, which are constantly monitored and improved. Those objectives must drive information security tactical decisions, just as the abovementioned principles guide strategic decisions. Continuous improvement is a key enabling factor in keeping the ever-increasing information security risks at bay and allowing the organisation to successfully accomplish its business objectives in the complex environment that surrounds it nowadays.

Approval and Ownership

Owner	Title	Date	Signature
Policy Author	Title	MM/DD/YYYY	
Approved By	**Title**	**Date**	**Signature**
Management Team	Title	MM/DD/YYYY	