Small Business Standards

SME GUIDE FOR THE IMPLEMENTATION OF ISO/IEC 27001 ON INFORMATION SECURITY MANAGEMENT

European DIGITAL SME Alliance

Chairman:
Fabio Guasconi

Coordinator:
Guido Sabatini

Experts:

Georgia Papadopoulou

George I. Sharkov

David Bulavrishvili

Sergio Oteiza

Holger Berens

Ermal Çifligu

Sebastiano Toffaletti

Nanuli Chkhaidze

Yuri V. Metchev

Thorsten Dombach

Alexander Häußler

FOREWORD

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. SBS was established in 2013 to meet the European Union's aspiration to make the standardisation system as inclusive, transparent and open as possible in line with Regulation 1025/2012 on the European Standardisation System.

The European DIGITAL SME Alliance (DIGITAL SME) is the continent's largest network of ICT small and mediumsized enterprises, representing around 20,000 digital SMEs. DIGITAL SME is a member of SBS and is a joint effort of 28 national and regional SME associations from EU Member States and neighbouring countries to put digital SMEs at the centre of the EU agenda.

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

This Guide was developed by the DIGITAL SME "WG27K" working group. The WG27K is made up of experts familiar with standardisation issues for information security management system and they fully understand SMEs' needs in this field. These experts were proposed by SME organisations from different EU countries and their selection was based on their competencies, to ensure the group's compositional diversity. SBS and DIGITAL SME are the sole proprietors of this free and publicly available Guide.

TABLE OF CONTENTS

1. Introduction to cybersecurity

Nowadays information is a core product for the majority of organisations, and for many – it's the only product. Other organisations heavily depend on processing information for their business purposes.

Yet there are people with malicious intentions, trying to manipulate the need for information to their own benefit. We have recently witnessed many examples of their illegal behaviour, such as viral ransomware attacks (WannaCry, Petya), leaks of personal data from large corporations (e.g. Equifax), and leaks of intelligence agencies' spying tools.

As the number of threats increases, organisations are obliged to think more about ways of protecting the information they handle, 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 complexity of the information environment and the intricacies of information flows, many organisations now understand the need for dedicated staff, such as information security managers, cybersecurity professionals, and information security committees. Some are also establishing specific departments/teams for information security and cybersecurity incident response. Yet many organisations are unsure whether their investments in protection measures are worthwhile.

Deficiencies in cybersecurity can lead to serious problems, which can be mainly assigned to three main 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 for 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.

1.2 Terms and definitions

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.

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 has much in common with other major initiatives that organisations may undertake. Before starting any activity, it is a good idea to decide which form they should take, their timeframe and the personnel's involvement. The very first initiators involved should be a subject-matter expert and top management: they must set up the bases for all the other activities.

Implementing this first step requires the involvement of top management, who should be accountable for establishing the information security foundations. Responsibility for this task lies with the information security manager. System owners and information owners should also be kept updated on the progress of task development. We include below a detailed explanation of the staff who, within an SME, could be assigned a role for 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 (Responsible, Accountable, Consulted, Informed) roles suggested in brackets.

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

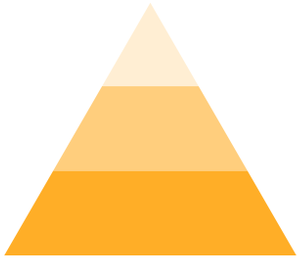
Even if information security concerns every department in the organisation, it is increasingly common to have an information security manager coordinating relevant activities. This role could be held by any high-ranking staff member (e.g. IT manager or Chief Technology Officer) with good knowledge of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

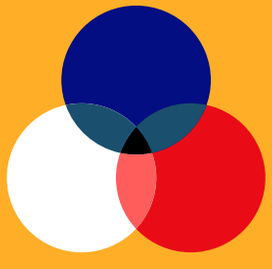
The information security manager is also usually responsible for promoting information security awareness, with other possible responsibilities including the establishment of communication channels and reporting. The success of information security depends greatly on communication, both internal and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

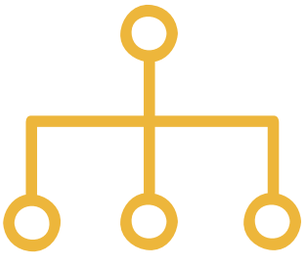
BENEFITS OF SETTING UP AN INFORMATION STEERING COMMITTEE:



Stronger coordination among different areas of the organisation



More effective spreading of an information security culture, as more departments are directly involved



Wider overview when making decisions, as all relevant areas depend on the committee

Establishing a routine to review and check information security status and development

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).

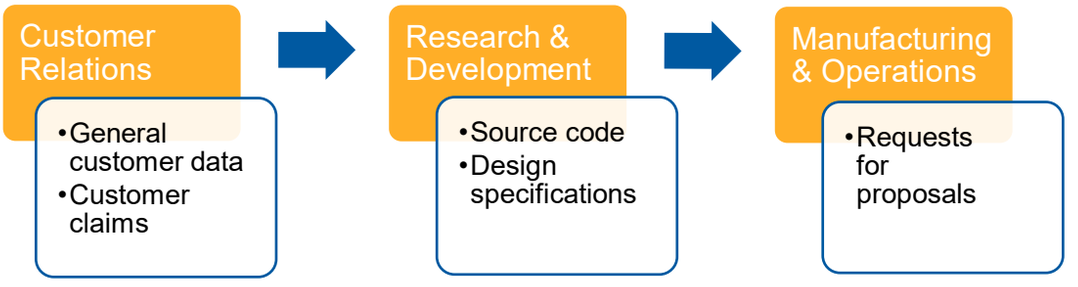
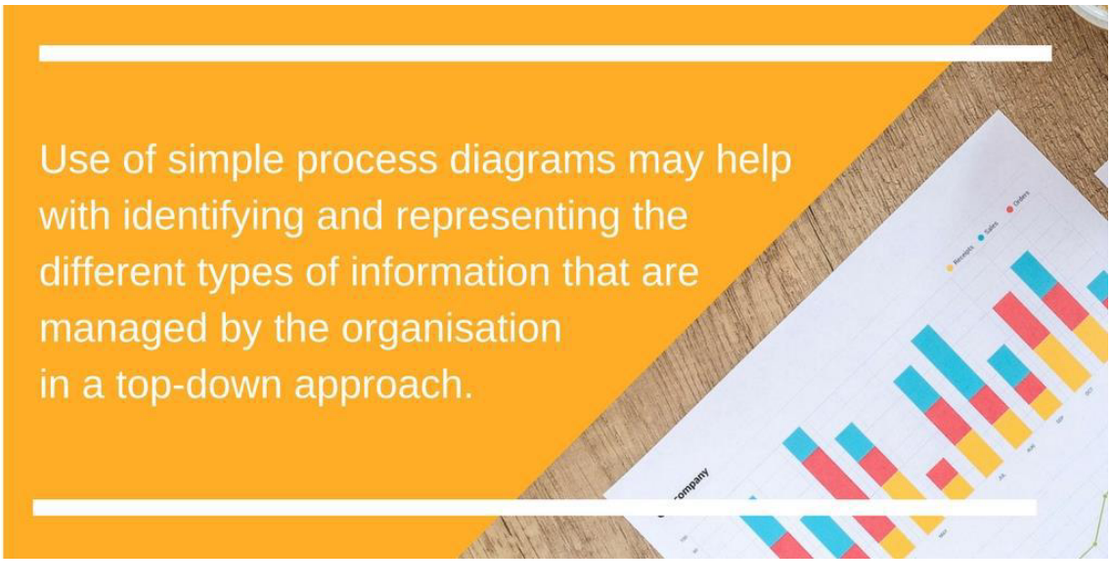


Figure 1: Example of asset map with reference to hypothetical information within a given organisation

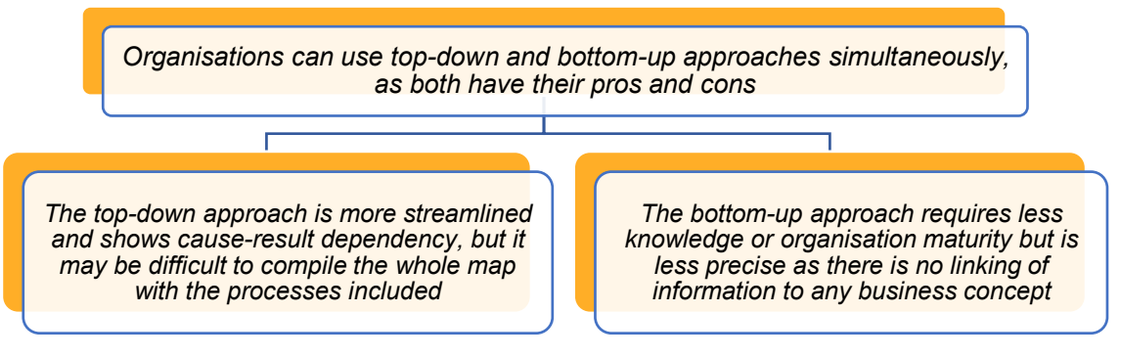
For the best use of a top-down approach, the organisation should have a good understanding of its processes, e.g. be aware of their nature, know who is responsible for each process, etc. The link between the organisation's activities and information can be made clear by starting with a bird's eye view 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	Production servers	Internal staff	Cloud provider	Main offices
ERP application	Testing servers		TLC provider	
Shared folders	Staff PCs			
	Staff smartphones			

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					
Production servers					
Testing servers					
Staff PCs					
Staff smartphones					
Shared folders					
ERP application					
Internal staff					
Cloud provider					
TLC provider					
Main offices					

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 (A)	Could the unavailability of this information significantly impact the organisation's business activities or reputation?	
	No	**Yes**
Confidentiality (C)	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
A: low C: high	A: low C: low	A: low C: high	A: low C: high	A: high C: low	A: low C: 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	
	A: low C: high	A: low C: low	A: low C: high	A: low C: high	A: high C: low	
CRM application						**A: low, C: high**
Production servers						**A: high, C: high**
Testing servers						**A: low, C: high**
Staff PCs						**A: high, C: high**
Staff smartphones						**A: low, C: high**
Shared folders						**A: low, C: high**
ERP application						**A: high, C: low**
Internal staff						**A: high, C: high**
Cloud provider						**A: high, C: high**
TLC provider						**A: high, C: high**
Main offices						**A: high, C: 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 much 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:

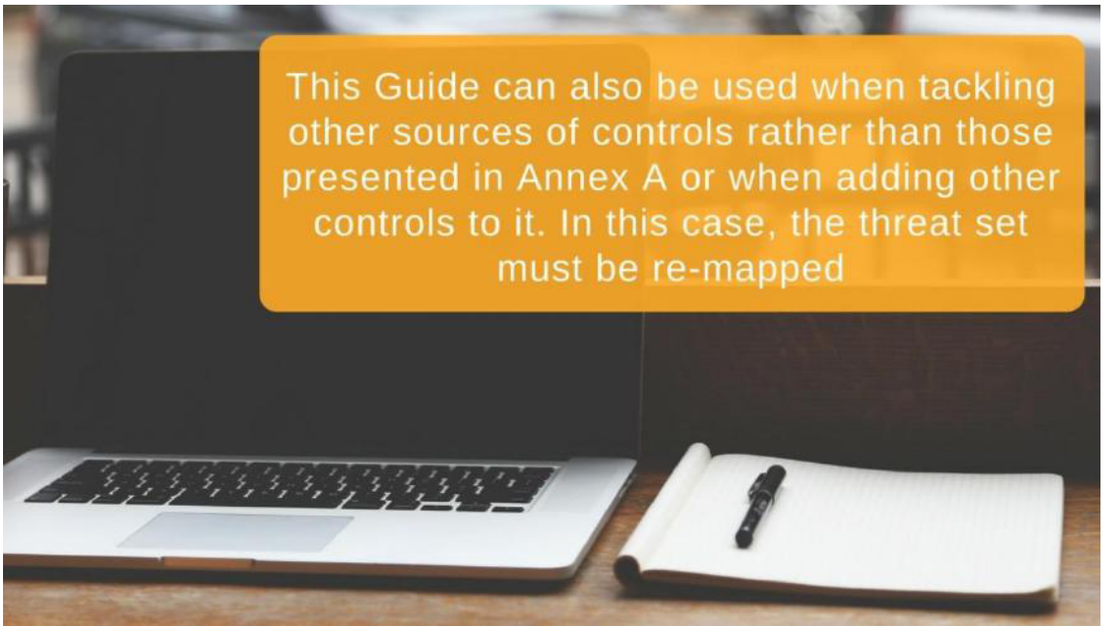
1) **baseline controls**, ideally to be implemented in every situation;
2) **discretionary controls**, which should be used to protect assets of high value, subject to likely threats.

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 'A:low, C: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.



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 interests.

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).

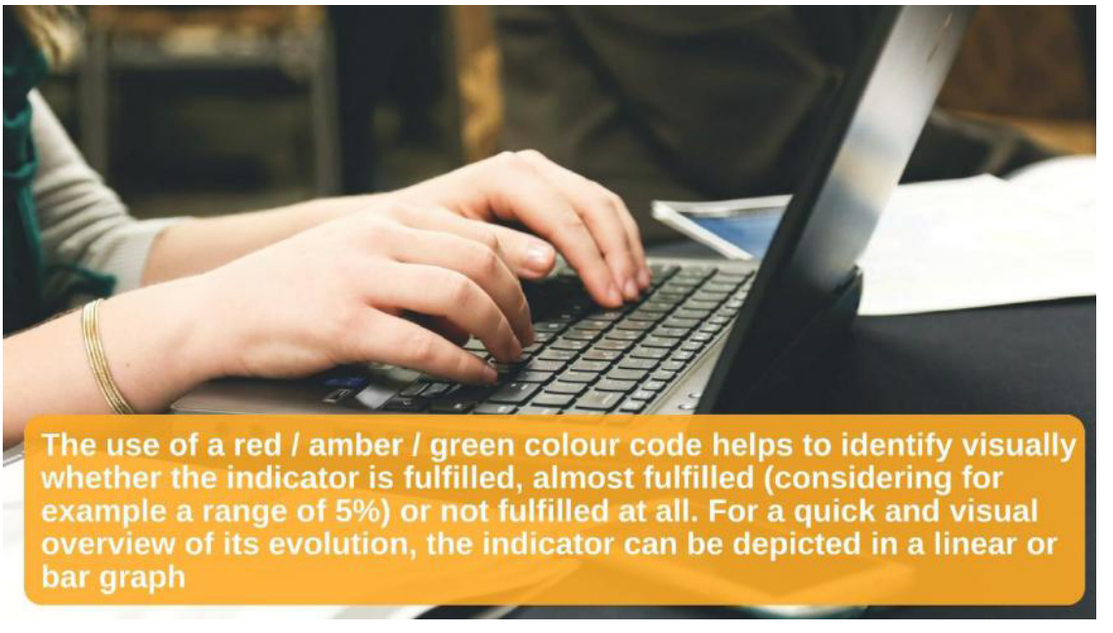
Non-conformities should be carefully analysed and actions implemented, thus avoiding their recurrence in the future. Such actions must be included in an updated version of the Information Security Plan, along with the actions necessary to correct non-conformities. Improvement opportunities should be 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 a 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.



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 1.2: 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

- CEN Workshop Agreement (CWA) 16458 on European ICT Professional Profiles. Available online at: ftp://ftp.cen.eu/CEN/Sectors/List/ICT/CWAs/CWA%2016458.pdf

Freely available 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://ccb.belgium.be/en/document/guide-sme

- European Union Agency For Network And Information Security (ENISA). *Information security and privacy standards for SMEs.* Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Available online at: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport

- ENISA. *Security guide and online tool for SMEs when going Cloud.* Available online at: https://www.enisa.europa.eu/news/enisa-news/enisa2019s-security-guide-and-online-tool-for-smes-when-going-cloud

- ENISA. *A simplified approach to Risk Management for SMEs*. Available online at: https://www.enisa.europa.eu/publications/archive/RMForSMEs

- ETSI. *NIS Directive Implementation – ETSI TR 103 456 – technical report released by ETSI's technical committee on Cybersecurity (TC CYBER)*. Available online at: http://www.etsi.org/deliver/etsi_tr/103400_103499/103456/01.01.01_60/tr_103456v010101p.pdf

- ISO. *Publicly available standards (including ISO/IEC 27000*). Available online at: http://standards.iso.org/ittf/PubliclyAvailableStandards/

ANNEX A

A.1 Baseline controls

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
01	**Information security policy**	5.1.1 5.1.2	An information security policy should be decided, agreed, published and communicated to all employees and to relevant third parties. The information security policy should be reviewed at a given frequency or in case significant changes occur to keep suitability, adequacy and effectiveness. *Suggested review frequency: annual*
02	**Information security organisation**	6.1.1 6.1.2	Roles and responsibilities of employees, contractors and any other party towards information security should be defined and documented while keeping duties and areas of responsibility segregated to limit damages arising from a single person's misbehaviour.
03	**Information security awareness, education and training**	7.2.2	All employees and relevant third parties should be periodically educated and made aware of information security threats. They should also be periodically trained according to the information security policy and procedures established by the organisation. *Suggested training frequency: yearly*
04	**Asset inventory**	8.1.1 8.1.2 8.1.3 8.1.4	A centralised asset inventory should be established, maintained and frequently reviewed. Ownership and responsibility for all assets should be identified, documented, accepted and implemented. A clear procedure for handling of all assets assigned to employees or a third party should be established and ensure traceability of those assets in all their lifecycle. *Suggested review frequency: monthly*
05	**Information classification, labelling and handling**	8.2.1 8.2.2 8.2.3	Information should be classified, labelled and handled according to its direct value for the organisation as well as to the current legislation. A procedure for information labelling and handling should be defined and applied by all information owners of the organisation. *Suggested classification levels: public, internal, confidential*
06	**User identification**	9.2.1 9.2.2	Information systems and services users should be uniquely identified through a formal registration and de-registration procedure for granting and revoking access.
07	**User authorisation**	9.2.3 9.2.5 9.2.6	The allocation and use of privileges to information systems and services users should be controlled and periodically reviewed. Users should only be provided with minimum rights needed to perform their duties. Any change of access privileges should be handled according to a strict procedure, subject to information owner's approval.
08	**User authentication**	9.2.4 9.3.1 9.4.1 9.4.2	Information systems and services users should be confidentially assigned credentials to authenticate themselves. Those credentials and the information systems verifying them should be robust enough to minimise the success of guessing attempts by

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
		9.4.3	unauthorised personnel. *Suggested credentials strength: 8 characters not from dictionary*
09	**Asset siting**	11.2.1 11.2.2 11.2.3 11.2.6	All assets carrying data or supporting information services should be sited in a way that is protected from accidental and environmental threats and always connected with adequate supporting utilities both if inside the organisation premises or outside them.
10	**Malware protection**	12.2.1	Malware protection software should be installed and kept constantly up-to-date on all assets that can be infected by malware.
11	**Information security procedures**	12.1.1	Information security procedures should be applied, documented, maintained, and be available to all users.
12	**Software vulnerability patching**	12.5.1 12.6.1	Security patches made available by vendors to overcome software vulnerabilities should be constantly evaluated and timely installed on all systems. *Suggested patching frequency: monthly*
13	**Network security**	13.1.1 13.1.2	ICT networks should be designed to limit the possibility for eavesdropping or altering the traffic, additionally limiting the authorised communications to the necessary ones while blocking all the others.
14	**Security in supplier agreements**	15.1.1 15.1.2 15.1.3	All suppliers with whom information are exchanged should be aware of the organisation's applicable security policies and be contractually bound to respect them, allowing verifications to be performed. This approach should also extend to their sub-contractors.
15	**Incident analysis and response**	16.1.2 16.1.3 16.1.4 16.1.5	All information systems and services users should note and report any observed or suspected security weaknesses for analysis. Specific incident response procedures should be activated depending on the analysis outcomes, while keeping full traceability of the evolving situation.
16	**Identification of legislation and contractual requirements**	18.1.1 18.1.4	All applicable information security requirements deriving from national, international or sectorial legislation should be kept under constant control as the ones deriving from contracts with third parties, with specific attention to personal data protection.

A.2 Discretionary controls

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
01	**External contacts and communications management**	6.1.3 6.1.4	The organisation should develop sufficient contacts with the authorities in order to swiftly react to widespread threats and with special interest groups, forums or associations mainly in order to get actual threat and control information.
02	**Remote working**	6.2.2	Remote working tools should be developed considering additional security protection to avoid information leaks and misuse. Remote accesses used for this purpose should be strengthened against unauthorised access
03	**Mobile device management**	6.2.1	Mobile devices used for working purposes should be securely configured and strictly controlled.
04	**Personnel screening**	7.1.1	All employees and third-party personnel regularly accessing the organisation's premises should have their criminal history and relevant background screened in accordance with relevant laws, regulations and ethics. The screening should be proportional to the business requirements.
05	**Personnel contract clauses**	7.1.2 7.2.3 7.3.1 13.2.4	All employees and third-party personnel should sign non-disclosure agreements before having any interaction with the organisation's information and their contract should require the respect of the organisation's information security policies. Consequences for disregarding those mandates, including after position changes or termination, should also be clearly defined.
06	**Removable media management**	8.3.1 8.3.3 13.2.1 13.2.2 18.1.3	Specific handling restrictions should be defined and implemented for all removable and portable media. Media containing information should be protected against unauthorised access misuse or destruction in case of transfer outside of the organisation's premises.
07	**Information disposal**	8.3.2 11.2.7	Strict procedures should be applied for the secure and safe disposal of media to be reassigned or dismissed in order to render previously stored data unrecoverable. *Suggested information disposal: full overwrite*
08	**Access control policy**	9.1.1 9.1.2	A formal access control policy covering the organisation's system and networks should be documented, maintained and reviewed in accordance with the security requirements, information classification and management and personnel authorisation levels.
09	**Encryption**	10.1.1 10.1.2	Cryptographic controls using strong algorithms should be developed, documented, implemented, maintained and reviewed to ensure confidentiality of confidential information transmitted and at rest. Cryptographic keys should be used, protected and kept according to strict and documented procedures during their whole lifecycle. *Suggested encryption algorithms: AES128+, SHA512+, RSA2048+*
10	**Physical security**	11.1.1 11.1.2	Physical protected barriers and secure areas to minimise unauthorised access to the organisation's premises and its

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
		11.1.3 11.1.6	information systems should be defined and equipped with access controls systems. Access points, including the ones for loading and unloading, should be minimised and equally secured.
11	**Environmental threats protection**	11.1.4	Physical protection against damages from natural causes or any other kind of natural or man-made disaster should be designed and applied to premises and information systems within them, starting from fire, humidity and earthquake protections. *Suggested threats to consider: fire, humidity, earthquake*
12	**Equipment maintenance**	11.2.4	All items of equipment should be maintained in the context of the Information Security Plan of the organisation. Maintenance access to information systems should be controlled.
13	**Unattended workplace and equipment**	11.2.8 11.2.9	Unattended equipment should be always left with the appropriate protection against physical unauthorised access and theft. All sessions should be locked when leaving any equipment and disconnect automatically after a defined inactivity period. No media should be left unattended in a workplace. *Suggested session timeout/screen saver: 15 minutes*
14	**Change management**	12.1.2 12.6.2 14.2.2 14.2.4	All changes to the organisation, business and information processes or systems that affect information security should be registered, duly approved and tested. System and software modifications should be allowed only to authorised personnel.
15	**Separation of development and test environments**	12.1.4 14.3.1	Development, test and operational facilities should be as much separated as possible to reduce the risks of unauthorised access or changes to the operational system. Data used for development and testing should additionally be different from production ones (anonymised or not related to real persons/facts). *Suggested separation: different systems and networks*
16	**Backup**	12.3.1	Backup copies of information and software should be created and tested regularly in accordance with a defined backup policy. *Suggested backup frequency: daily/weekly*
17	**Event logging and storage**	12.4.1 12.4.2 12.4.3	Event logging records of most security-relevant operations should be produced, securely stored, protected from both access and modifications and regularly reviewed. All system administrator and system operator activities should be logged as succeeded and attempted login/logouts. *Suggested log retention: 6 months+*
18	**Time synchronisation**	12.4.4	System clocks should be constantly synchronised in all areas of the organisation or in a security domain with an agreed and reliably accurate time source.
19	**Network segregation**	13.1.3	Information services, users, and information systems should be segregated within different network areas with homogeneous security requirements. The segregation should be performed using firewalls or equivalent devices.
20	**Messaging security**	13.2.3	Information transferred via electronic messaging and the supporting systems should ensure confidentiality and detect attacks through these channels.

ID	Control name	ISO/IEC 27001 Annex A ref.	Control description and guidance
21	**Security by design**	6.1.4 14.1.1 14.2.5	Information security should represent an integral part of information systems across their entire lifetime, starting from the requirements for information systems early design. All the organisation's projects should include information security considerations as early as possible.
22	**Application services security**	14.1.2 14.1.3	Information systems used to provide services should be protected against common attacks through a secure and hardened configuration, developed to use additional security controls and constantly monitored/protected through security dedicated devices proportionally to their exposure. *Suggested security devices: firewalls and IDS/IPS*
23	**Secure development lifecycle**	14.2.1 14.2.6 14.2.7	Organisations should establish secure development lifecycle criteria for their applications, to be applied also for external custom projects in order to minimise applications' vulnerabilities.
24	**Security testing**	14.2.3 14.2.8 14.2.9 18.2.3	Security and acceptance criteria for new information systems, upgrades and new versions should be established and suitable tests of the system carried out during development, prior to acceptance and periodically thereafter, requiring previous fixing of discovered vulnerabilities. *Suggested periodicity: every 6 months internal, every quarter external*
25	**Suppliers security monitoring**	15.2.1 15.2.2	The implementation of changes to supplier services should be monitored, controlled and reviewed by the use of formal change control procedures. The respect of security clauses and security service levels should be constantly monitored.
26	**Incident management policy**	16.1.1	Information security incidents should be controlled, registered, handled and addressed according to specific responsibilities approved and established by the management. Appropriate communication and escalation procedures should also be established.
27	**Incident lesson learned**	16.1.6	Knowledge gained from analysing and resolving information security incidences should be used to reduce the likelihood or impact of future incidents possibly adapting incident response procedures.
28	**Redundancy management**	17.2.1	Information processing facilities should be implemented with redundancy sufficient to meet availability requirements also in failure situations.
29	**Intellectual property protection**	18.1.2	Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material covered by intellectual property rights and on the use of proprietary software products.
30	**Information security assessments and audits**	18.2.1 18.2.2	Information security systems should be regularly reviewed by independent auditors. Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards. Information systems should be regularly reviewed to provide continuous compliance with security implementation standards.

A.3 Discretionary controls threat relationship (mitigation)

ID	Control	Physical attack	Unintentional damage	Disaster	Failures-malfunction	Outages	Eavesdropping-interception-hijacking	Legal	Nefarious-activity-abuse
A2.01	External contacts and communications management	Secondary		Primary		Secondary	Primary		Secondary
A2.02	Remote working			Secondary		Secondary	Primary		
A2.03	Mobile device management	Secondary	Secondary	Secondary		Secondary	Primary		Secondary
A2.04	Personnel screening				Secondary		Primary	Primary	Secondary
A2.05	Personnel contract clauses	Secondary	Secondary		Secondary		Primary	Primary	Primary
A2.06	Removable media management	Primary	Primary	Secondary	Secondary	Secondary	Primary	Secondary	
A2.07	Information disposal	Secondary	Secondary		Secondary		Primary		
A2.08	Access control policy						Primary		Primary
A2.09	Encryption						Primary	Primary	
A2.10	Physical security	Primary	Secondary				Primary		
A2.11	Environmental threats protection	Primary	Secondary	Primary		Primary	Secondary		
A2.12	Equipment maintenance	Primary	Primary		Primary	Secondary			
A2.13	Unattended workplace and	Secondary					Primary		

ID	Control	Physical attack	Unintentional damage	Disaster	Failures-malfunction	Outages	Eavesdropping-interception-hijacking	Legal	Nefarious-activity-abuse
	equipment								
A.2.14	**Change management**		Secondary		Secondary		Primary		Secondary
A.2.15	**Separation of development and test environments**				Secondary		Secondary		
A.2.16	**Backup**	Primary	Primary	Primary	Primary	Secondary		Secondary	Secondary
A.2.17	**Event logging and storage**		Secondary		Secondary		Primary	Secondary	Primary
A.2.18	**Time synchronisation**		Secondary		Secondary		Primary	Secondary	Primary
A.2.19	**Network segregation**		Secondary			Secondary	Primary		Secondary
A.2.20	**Messaging security**		Secondary				Primary	Secondary	Secondary
A.2.21	**Security by design**		Secondary		Secondary	Secondary	Primary		Primary
A.2.22	**Application services security**		Secondary				Primary	Secondary	Primary
A.2.23	**Secure development lifecycle**		Primary				Primary		Secondary
A.2.24	**Security testing**		Secondary				Primary		Primary
A.2.25	**Suppliers security monitoring**				Secondary	Primary		Secondary	
A.2.26	**Incident management policy**	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary
A.2.27	**Incident lesson learned**	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary	Secondary
A.2.28	**Redundancy management**			Primary	Primary	Primary		Secondary	Primary

ID	Control	Physical attack	Unintentional damage	Disaster	Failures-malfunction	Outages	Eavesdropping-interception-hijacking	Legal	Nefarious-activity-abuse
A.2.29	Intellectual property protection							Primary	
A.2.30	Information security assessments and audits		Secondary				Secondary	Primary	Secondary

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 be always proportionate to the risks it must counter;
2) all accesses 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 to keep the ever-increasing information security risks at bay and to allow 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	

European Commission

EFTA

Small Business Standards

European DIGITAL SME Alliance

sbs-sme.eu
@SBS_SME

digitalsme.eu
@EUdigitalsme

Co-financed by the European Commission and EFTA