Small Business Standards

SME Guide on Information Security Controls

European DIGITAL SME Alliance

This guide was developed by an ad-hoc group created by experts of the SBS working group Digitalisation and DIGITAL SME working groups Standards and Cybersecurity and Data Protection. The ad-hoc group was made up of standardisation experts familiar with cybersecurity issues that fully understand SMEs' needs in this field.

Chairman:
Jean-Luc Allard

Coordinator:
Omar Dhaher

Experts:

Andrea Caccia

Daniele Tumietto

Davide Giribaldi

Francisco Menéndez

Samuel Fricker

Published:
April 2022

ABOUT THIS GUIDE

Small Business Standards (SBS) is the association representing European small and medium-sized enterprises' (SMEs) interests in standardisation at the European and international levels. Its main goals are derived from Regulation 1025/2012 on European standardisation. SBS aims to increase SMEs' awareness and influence in standardisation. It does this by facilitating the uptake of standards by SMEs, representing their interests, and motivating them to engage in the standardisation process.

The European DIGITAL SME Alliance (DIGITAL SME) is a member of SBS. It is the continent's largest network of ICT SMEs, representing around 45,000 digital SMEs.

In its efforts to raise awareness and help SMEs adopt and use cybersecurity standards, SBS issued an SME guide on ISO/IEC 27001 in 2017. Recognising the rising need for SMEs to adhere to cybersecurity requirements and to build their technical capacity in this regard, SBS has developed this guide on ISO/IEC 27002 on Information Security Control for SMEs.

SBS is the sole proprietor of this free and publicly available guide.

List of Acronyms

BYOD: Bring Your Own Device
CEO: Chief Executive Officer
CERT: Computer Emergency Response Team
COBIT: Control Objectives for information and related technologies (ISACA.org)
DAC: Discretionary Access Control
DTG: Date-Time Group
DPO: Data Protection Officer
EGIT: Enterprise Governance of Information and Technology
GDPR: General Data Protection Regulation
IEC: International Electrotechnical Commission
ICT: Information and Communications Technology
IoT: Internet of Things
IP: Internet Protocol
ISMS: Information security management system
ISO: Information Security Officer
ISO: International Organization for Standardization
LAN: Local Area Network
MAC: Mandatory Access Control
OS: Operating System
PII: Personally Identifiable Information
PIMS: Privacy information management system
RACI : RACI a management assignment matrix. The acronym stands for:
Responsible, the people who are in charge to do the job
Accountable, the person who is ultimately responsible to achieve the objectives and report to the top management
Consulted, the people whose advice is searched to select the objectives and define the activities, and
Informed, the people who should be put aware of the activities and expected results.
VPN: Virtual Private Network
WAN: Wide Area Network

TABLE OF CONTENTS

1. INTRODUCTION 6

2. SCOPE 7

3. DEFINITIONS 7

3.1 General definitions 7

3.2 Privacy definitions 9

3.3 Security definitions 10

4. WHY DO SMES NEED TO PROTECT INFORMATION? 10

4.1 Differences between information and ICT security 12

4.2 Influence of Internet and cyber aspects 13

5. PRIVACY PROTECTION 13

5.1 Main concepts 13

5.2 Privacy-related certifications 14

5.3 Privacy controls 15

6. INFORMATION SECURITY GOVERNANCE 16

6.1 What is Information Security Governance? 16

6.2 ISO/IEC 27014 17

6.3 COBIT 17

7. CONTROLS FOR INFORMATION SECURITY AND PRIVACY PROTECTION 19

7.1 Introduction 19

7.2 Controls 20

CONTROL #1: ASSET MANAGEMENT 21

CONTROL #2: POLICIES, STANDARDS, AND GUIDELINES 24

CONTROL #3: INCIDENT MANAGEMENT 25

CONTROL #4: ACCESS CONTROL MANAGEMENT 28

CONTROL #5: NETWORK SECURITY AND DATA EXCHANGES 31

TABLE OF CONTENTS

CONTROL #6: VULNERABILITY MANAGEMENT 33
CONTROL #7: FIGHTING MALWARE 34
CONTROL #8: BACKUP MANAGEMENT 35
CONTROL #9: SAFEGUARDS MANAGEMENT 36
CONTROL #10: ICT READINESS FOR BUSINESS CONTINUITY 38
CONTROL #11: REMOTE WORKING 43
CONTROL #12: CYBERTHREATS WATCH 45
CONTROL #13: INFORMATION SECURITY AWARENESS 47
CONTROL #14: INFORMATION SECURITY ASPECTS IN RELATIONS TO SUPPLIERS 49
CONTROL #15: INFORMATION SECURITY ORGANISATION 51
CONTROL #16 ADDITIONAL PRIVACY CONTROLS 55
8. CONCLUSION 58
ANNEX A: INFORMATION CLASSIFICATION TECHNIQUE 60
ANNEX B: LISTING OF THE CONTROL TITLES WITH THEIR NUMBER, PER REFERENCE 68
ANNEX C: COBIT PROCESSES AND SECURITY MANAGEMENT 70
ANNEX D: A LIST OF COMPUTER EMERGENCY RESPONSE TEAM (CERTS) 74
BIBLIOGRAPHY 75
ABOUT THE EXPERTS 77

1. INTRODUCTION

Digital transformation is playing an important role in restructuring businesses around the globe. Enabling technologies such as 5G, Artificial Intelligence, Blockchain, Edge Computing, and the Internet of Things (IoT) are the heart of this transformation. Recognising its strategic role for the EU long term objectives, the European Commission has developed its 2030 Strategy – the DIGITAL Decade – that includes the following objectives:

1. 75% of European enterprises to take up cloud computing services, big data, and Artificial Intelligence;
2. More than 90% of European SMEs to reach at least a basic level of digital intensity;
3. Grow the number of scale-ups and finance to double EU Unicorns;

Digital SMEs are providing innovative solutions in fields such as 5G, IoT, Edge Computing, to enable other businesses to reach digital competencies and achieve digital transformation. In this framework, security remains a crucial topic in the uptake of enabling technologies and solutions businesses need.

Cybersecurity is a requirement across the whole supply chain to ensure a smooth transformation of industrial processes from physical to cyberspace[1]. Since 99% of European enterprises are SMEs, protection from cyber-attacks becomes crucial for Europe's economy.

However, the adoption of ICT and information security is low. In 2019, Eurostat estimated that 33% of EU enterprises have documents on measures, practices, or procedures on ICT security, while 24% of EU enterprises defined or reviewed ICT security documents within the last 12 months.

1 SBS (2020, page 3), EU Cybersecurity Act and the role of standards for SMEs

Cybersecurity standards can help enterprises to adhere to a set of requirements that provide a necessary and basic layer of protection. However, such requirements remain complex and costly for SMEs to implement. By 2020[2], there were around 32000 certificates for ISO/IEC 27001 Information Security Management System worldwide, while there are around 190 million enterprises operating globally.

The guide is written by SME owners and professionals working in or for SMEs with accumulated experience and knowledge of the security challenges that most small businesses face on a daily basis. It is composed of two main parts. The first part explains the need for a clear strategy and objectives for an efficient implementation of security controls and introduces basic concepts of privacy and their relevance to security controls, certifications, and compliance with GDPR. The second part recommends the minimum essential controls that SMEs need to implement to protect their information and be compliant with GDPR rules.

2. SCOPE

The scope of this guide is information security in the broadest sense. The guide targets both the SME's management (CEO and DPO) and technical teams (SME cybersecurity provider, cybersecurity practitioners/experts) and ICT SMEs. For the SME's management, the guide aims to raise awareness of the issues faced by SMEs and to help managers to take the lead in the activities that their technical staff or security providers should carry out. The guide raises awareness regarding issues related to:

- Importance of protecting information (Section 4),
- Privacy protection and compliance with GDPR (Section 5)
- Information Security Governance (Section 6)
- Information Security Controls (Section 7.1)

Information security risk management is not directly addressed as it is not a control. This topic is dealt with in the SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management.

SMEs with adequate cybersecurity skills and awareness[3] can then proceed with section 7.2, which provides an overview of the selected 16 controls, deemed essential for any SME to protect its information and comply with GDPR rules. The guide intends to support the transformation of SMEs that wish to become aware of "cybersecurity-capable with awareness of proper cybersecurity practices". Technical teams and cybersecurity SMEs can refer to the controls presented in section 7 to ensure optimal implementation of security measures for SMEs' infrastructure.

SMEs including micro businesses that do not have a dedicated DPO or security professionals are highly advised to seek help from cybersecurity SMEs and/or practitioners to ensure proper protection of their data.

3. DEFINITIONS

3.1 General definitions

Business Continuity (BC): Refers to maintaining core business functions of the entire organisation or quickly resuming them in case of disruption like an attack from cybercriminals.

Business continuity plan: A set of procedures and instructions that an organisation must follow to

2 SBS (2020, page 4), EU Cybersecurity Act and the role of standards for SMEs

3 Shojaifar and Järvinen (2021, page 3), An SME that falls under the columns (CSTA and GSGP) would be able to continue with section 7.2. Other SMEs need help from other Cybersecurity SMEs or professionals to implement controls in section 7.2. Click here for more information on Shojaifar and Järvinen's framework.

promptly react to an incident. A business continuity plan covers business processes, assets, human resources, business partners and all stakeholders involved in the company's ecosystem.

Business impact analysis: It is another core part of a BC plan. It identifies the impact of business loss (usually quantified in costs) and helps to look at the entire organisation's processes and to evaluate them, determining which are most important.

Control: Measure (process, policy, device, practice or action) that is modifying risk.

Confidentiality: Property that information is not made available or disclosed to unauthorised individuals,

entities, or processes.

Disaster recovery plan: An important part of a BC plan, but it is not the plan itself. It focuses mainly on restoring an IT infrastructure and all related operations after an incident.

Governance of Information Security: System by which an organization's information security activities are directed and controlled.

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

Information Security risk: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organisation. (Note 6 to 3.61)

Information System: Set of applications, services, information technology assets, or other information-handling components.

Integrity: Property of accuracy and completeness.

Policy: Intentions and direction of an organisation, as formally expressed by its top management.

Process: Set of interrelated or interacting activities which transforms inputs into outputs.

Risk management: coordinated activities to direct and control an organisation regarding risk.

3.2 Privacy definitions

The following definitions are in line with GDPR. ISO/IEC 27701 and in general the ISO standards use the term "Personally Identifiable Information (PII)" where the term "personal data" is used in GDPR. Hence, the guide will use the term "personal data".

Personal data: Any information relating to an identified or identifiable natural person.

Data subject: An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Personal data processing, or Processing: Any operation or a set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.

Controller: The natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processor: A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

3.3 Security definitions

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

Confidentiality: Property that information is not made available or disclosed to unauthorised individuals, entities, or processes.

Documented information[4]: Information required to be controlled and maintained by an organisation and the medium on which it is contained.

Information Security event: Identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that can be security relevant.

Information Security incident: Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Likelihood: Chance of something happening.

Malware: A wide range of malware types exists:

- **Virus:** Replicates itself in executable files.
- **Worm:** Travels through the communication channels via one's contacts.
- **Spyware:** Monitors your activities and sends information to a hacker's server.
- **Ransomware:** Freezes your system by encrypting files and the hacker promises to give you access back after having paid a ransom.
- **Logic bomb:** Rests silently in your system until specific programmed conditions occurs, when it burst out causing fatal damage.
- **Trojan (horse):** Included in benign software that you bought or downloaded, and that performs several hidden activities.

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

4. WHY DO SMES NEED TO PROTECT INFORMATION?

Information is probably the most crucial asset for any organisation, including SMEs. What can an organisation do if the information is unreliable or already in the hands of one who can block you, or modify data without you knowing it? Or, simply what if information is not available or accessible when you need it? Is all information accessible on the internet trustable?

Most of us know ISO 9001, the famous Quality Management System. Do you know the existence of ISO/IEC 27001 that addresses the Information Security Management System? Its first publication dates back to 2005 and its structure and content are very similar to ISO 9001. If you have implemented the first standard, you can implement the second one without much effort. Refer therefore to the "SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management"

However, it requires understanding of the scope and the need behind it. What is information? Why do we need to protect it? What is the link with GDPR? These are the questions this guide intends to answer.

4 Note 1 to entry: Documented information can be in any format and media and from any source. Note 2 to entry: Documented information can refer to the management system including related processes, information created in order for the organisation to operate (documentation), and evidence of results achieved (records).

What is information?

Information is (a set of) interpretable data that, within a given context, has (have) a signification and a value. To ensure and enhance this value data, interpretability and context need to be preserved and protected.

Why? Simply because without information and more specifically - trustable information - very few is achievable in our life. Human beings – and even more naturally and unconsciously our body – do nothing else other than handling data and information all the time: for example, preparing bread, driving a car, and healing a physical problem. Information is intertwined with any human activity.

Information is essential as it serves to:

- increase our knowledge and skills. (We all know that knowledge gives us power[5] over those who do not have it);
- make good decisions;
- act to realise our objectives;
- measure our achievements.

What if the used information is not trustable because it is

- already in the hands of the ones who can prevent us from achieving our objectives (confidentiality)?
- modified in an uncontrolled way in any of the phases of its handling (integrity)?
- unavailable and unreachable when we need it (availability)?

What is information security?

Confidentiality, integrity, and availability have long been described as the three main security criteria for information security. Compliance with laws and regulations, where the processing of personal data is

5 Power 1: Of the one who knows about the ignorant; Power 2: Knowing something about someone else and using it to get something (blackmail); Power 3: Preventing one to access the information needed (deactivate the person).

definitely one of the most relevant issues to be addressed, is increasingly becoming a priority for SMEs, if only because of the sanctions involved.

The two 'key' standards on information security are ISO/IEC 27001 (Information Security Management System – ISMS) and ISO/IEC 27002 (Code of Practice for information security control). Applying ISO/IEC 27001 on Personally Identifiable Information (PII) also directly enhances the level of compliance with General Regulation on Data Protection (GDPR) although it does not directly ensure it, but there is now ISO/IEC 27701, a specific standard addressing this.

However, sophisticated management of the used information is required. ISO/IEC 27002 is a list of 114 controls to ensure information security. These are generally determined, especially for their implementation in each context, within a risk management process as explained in ISO/IEC 27005.

GDPR requires controlled management of Personal Identifiable Information, which is a category of information handled by any SME: these relate to their personnel, clients, and providers as soon as the name of a person is associated with anything else. Here, ISO/IEC 27001 and 27002 are also applicable and completed by ISO/IEC 27701.

The information security risk assessment process shall also identify risks related to the processing of personal data and, in particular, with the loss of confidentiality, integrity and availability of personal data. The controls and other recommendations in this guide are aimed to reduce the assessed risks. More information on the risk management process can be found in the SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management.

Why do we need standards for this?

Recent and forthcoming European laws and regulations consistently rely on the accountability principle and a risk-based approach, especially for new technologies that are particularly relevant for start-ups. The complexity and cost of compliance without a sound structured approach can quickly become unmanageable for any organisation and standards represent a recognised solution to address this.

Anyone speaking the language of the society in which he/she lives uses two de facto standards to understand the situations and to be understood: spelling and grammar. Thus, standards for information security help us to better implement actions in accordance with regulations, manage each entity's unique situation and increase competitiveness.

Information security standards are the responsibility of Sub Committee 27 of the Joint Technical Committee 1 within ISO and IEC (International Electrotechnical Committee), known as ISO/IEC JTC 1 SC 27: Information Security, Cybersecurity and Privacy Protection.

Standards are developed for enterprises of all sizes. However, identifying suitable ones and adapting them for use, especially for SMEs, can be a barrier to their use. This document aims to be a guide in the selection and adaptation of standards for SMEs.

4.1 Differences between information and ICT security

Information security addresses the protection of information regardless of the media (physical, spoken, or projected, and on digital media and systems). ICT security deals with the protection of ICT systems and the data they contain and process.

4.2 Influence of Internet and cyber aspects

Internet and, more widely, cyberspace bring many opportunities along with new and permanently evolving vulnerabilities and risks. This is the reason why this guide contains helpful guidance on network and cyber security.

5. PRIVACY PROTECTION

5.1 Main concepts

The GDPR lays down rules with regard to the processing of personal data and rules relating to the free movement of personal data (Art. 1). The goal is to protect the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

This process is usually associated with the term 'privacy protection'.

Every business needs to process personal data for its proper functioning. Therefore, any European SME has to properly address the issue of GDPR compliance. This document provides basic guidance on GDPR compliance, based on ISO/IEC 27701, a standard that extends ISO/IEC 27001 and 27002 providing requirements and guidelines for privacy information management. This makes the approach sound and, when needed, lays the groundwork also for compliance in other jurisdictions.

However, it should be considered that this document does not aim to be exhaustive but to help SMEs to adopt the most important controls. For this reason, also considering the sensitivity of the subject and the high fines in case of non-compliant processing, it is always necessary to check the text of the GDPR. Especially when the processing of personal data is part of the core business of the SME, it is strongly recommended to read and apply ISO/IEC 27701, for which this guide can be a useful introduction.

When the SME is implementing a type of processing that is likely to result in a high-risk situation to the rights and freedoms of natural persons, it shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (See GDPR Art. 35 for further details). An additional tool is a certification foreseen in Art. 42 and 43 of GDPR and described in Section 5.2. When

established, it will be a useful tool to reduce the risk of non-compliance.

5.2 Privacy-related certifications

The ISO/IEC 27001 standard supports a third party certification as an information security management system, therefore a Certification Body that operates under accreditation and certifies compliance with this standard shall be accredited according to ISO 17021-1:2015, a standard that specifies "principles and requirements for the competence, consistency and impartiality of bodies providing audit and certification of all types of management systems"[6].

Art. 42 of Regulation (EU) 2016/679 encourages the establishment of data protection certification mechanisms to demonstrate compliance with the GDPR of the processing carried out by data controllers and processors.

In addition, Art. 43 establishes the characteristics of the Certification Bodies that will certify the compliance of personal data processing with the GDPR; these Bodies have to be accredited either by the Supervisory Authority or by the national accreditation body in accordance with ISO/IEC 17065:2012, which defines the requirements for the competence, consistent operation, and impartiality of certification bodies for products, processes, and services.

ISO/IEC 27701 is an extension of ISO/IEC 27001 so it requires that the certification body is accredited according to ISO 17021-1:2015, like for ISO/IEC 27001. Therefore, it is not possible to use ISO/IEC 27701 as a basis for an articles 42 compliant certification because article 43 requires that the certification body is accredited with ISO/IEC 17065:2012.

Therefore, while GDPR (Regulation (EU) 2016/679) requires a 'product' type certification to demonstrate GDPR compliance, ISO/IEC 27701 is certifiable as an extension of ISO/IEC 27001 and requires a 'management system' type certification.

In order to unravel this bundle that has been created between ISO/IEC 17021 and ISO/IEC 17065, it is desirable that the European Data Protection Board (EDPB) is able to declare valid or not the certification according to the ISO/IEC 27701:2019 extension. This is the only way to maintain one of the key principles on which the GDPR is based: equal rules for data processing in all EU member states.

Organisations that have already implemented an ISMS (Information Security Management System) according to ISO/IEC 27001 can extend it to privacy management, including the processing of personal data, using ISO/IEC 27701.

6 All certifying organizations MUST be accredited otherwise, the ISMS/GDPR certificate is not valid and recognized. Certification shows compliance (for a period of 3 years). Certification is not compulsory but voluntary. Most organizations (and SMEs) choose for an implementation that is verified by a trusted third party.

Organisations that do not have an ISMS can also implement ISO/IEC 27001 and 27701 together in a single project, as ISO/IEC 27701 simply extends the requirements provided by 27001 and its 'code of conduct' (ISO/IEC 27002). It is therefore not necessary to carry out two separate certifications.

A certification based on ISO/IEC 27701 is an internationally recognised tool that can help to demonstrate compliance with data protection legislation, even if it is not strictly in line with the GDPR Art. 42 certification.

This is all pending clarification of the potential of ISO/IEC 27701 as a means of demonstrating compliance with the GDPR of personal data processing carried out either as a data controller or as a data processor.

In any case, an ISO/IEC 27701-compliant Privacy Information Management System (PIMS) is useful for any organisation with data protection obligations. It is of particular interest to organisations that operate internationally, work with customers in other jurisdictions or operate in international supply chains. These organisations are often required to comply with a variety of privacy regulations and laws, and this new standard can simplify addressing conformance.

By implementing a PIMS as an extension of an existing ISO/IEC 27001-compliant ISMS, an organisation can collect and process data, including personal data, in a systematic way. They can also manage the risks associated with the confidentiality, integrity, and availability of the information, and respond to evolving threats and risks to that data and privacy.

A PIMS also enables organisations to reduce the costs associated with privacy and information security by constantly adapting to changes in both the environment and within the organisation, increasing resilience to cyber-attacks.

A PIMS has several advantages:

- Building confidence in your company's ability to manage personal information, both for customers and employees.
- Assisting in demonstrating compliance with GDPR and other applicable privacy regulations.
- Clarifying roles and responsibilities within your organisation.
- Improving internal competence and processes to avoid breaches.
- Providing transparency on established privacy management controls.
- Facilitating agreements with business partners where the handling of PII (personally identifiable information) is mutually relevant.
- Easily integrating with the main standard for information security ISO/IEC 27001.

ISO/IEC 27701 provides a set of annexes that assist in the development of appropriate controls, both for implementing the necessary security and compliance measures and for developing risk assessments.

5.3 Privacy controls

ISO/IEC 27701 is a tool designed to correctly address security and risk management issues in relation to processing of personal data, and in doing so it "leans" on ISO/IEC 27001, creating value and the conditions for rapid integration. The same applies for ISO/IEC 27701 privacy controls that have been included in section 7, that describes both the most important information security and privacy controls based on ISO/IEC 27001 and ISO/IEC 27701.

For each control, a specific subparagraph (Extension to privacy) is added when a general control defined in ISO/IEC 27001 is specialised by ISO/IEC 27701. Specific and additional privacy controls are described at the end of section 7 (Controls 14-16).

6. INFORMATION SECURITY GOVERNANCE

6.1 What is Information Security Governance?

Governance of information security is the use of resources to ensure effective implementation of information security, and provides assurance that:

- directives concerning information security will be followed; and
- the governing body will receive reliable and relevant reporting about information security-related activities.

The implementation of security controls without a clear strategy and objectives can lead to them being inefficient and even detrimental to the organisation. For this reason, enterprise governance is essential. IT governance directing the implementation of information and communication technologies and information security governance guiding information management are both components of enterprise governance.

Enterprise Governance of Information and Technology (EGIT) is complex and multifaceted. As such, members of the governing boards and senior management typically need to tailor their EGIT measures and implement it to their own specific context and needs.

Fundamentally, EGIT is concerned with value delivery from digital transformation and the mitigation of

business risk that results from it. More specifically, three main outcomes can be expected after the successful adoption of EGIT:

- benefits realisation
- risk optimisation
- resource optimisation.

6.2 ISO/IEC 27014

In relation to the governance of information security, the ISO/IEC 27014 standard establishes the strategy to be followed. It defines 6 objectives:

1. ensure an organisation-wide information security approach that is aligned with the business objectives;
2. ensure the decisions are made on a risk-based approach;
3. ensure the acquisition of products and services follow a defined process and direction [set the direction of acquisition];
4. ensure information security is compliant with internal and external requirements;
5. foster a security-positive culture;
6. ensure the security performance follows current and future requirements of the organisation.

These objectives can be achieved if a security governance strategy is established based on the following four processes:

1. evaluate
2. direct
3. monitor
4. communicate.

ISO/IEC 27014 differentiates between the governing body, which evaluates, directs and monitors; and the management body, in charge of implementing the ISMS through ISO/IEC 27001.

As usual in the standards, ISO/IEC 27014 tells us what to do but not how to do it; and specialised knowledge is needed to bring the strategy defined by the governing body to the concrete and measurable processes and procedures. This knowledge can be supplied by COBIT.

6.3 COBIT

What is COBIT?

COBIT (Control Objectives for Information and related Technology) is a framework for the governance and management of enterprise information and technology, including security issues, aimed at the whole enterprise. Enterprise I&T refers to all the information processing-related technology the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organisation, but certainly includes it.

The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organisational structures, and serve different purposes.

Governance ensures that:

- stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives;
- direction is set through prioritisation and decision making;
- performance and compliance are monitored against agreed-on direction and objectives.

Management plans, builds, runs, and monitors activities, in alignment with the direction set by the governance body, to achieve the enterprise objectives.

COBIT Structure:

For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved. The governance and management objectives in COBIT are grouped into five domains (1 under section A, and 4 under section B):

- A. Governance objectives are grouped in the Evaluate, Direct and Monitor (**EDM**) domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.
- B. Management objectives are grouped into the other four domains:
  - Align, Plan and Organise (**APO**) addresses the overall organisation, strategy and supporting activities for I&T;
  - Build, Acquire and Implement (**BAI**) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes;
  - Deliver, Service and Support (**DSS**) addresses the operational delivery and support of I&T services, including security;
  - Monitor, Evaluate and Assess (**MEA**) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

Why COBIT?

- Applying the COBIT methodology to information security provides several benefits, including:
- reduction of complexity and increased cost-effectiveness through improved and easier integration and alignment of information security standards, good practices and/or sector-specific guidelines;
- higher stakeholder satisfaction thanks to a better understanding of information security and its outcomes;
- better integration of information security across the enterprise;
- better-informed risk decisions and risk awareness;
- improvements in prevention, detection, and recovery;
- reduction—in terms of both impact and probability—of information security incidents;

- better support for innovation and competitiveness;
- better management and optimisation of costs related to information security;
- better understanding of information security by stakeholders.

7. CONTROLS FOR INFORMATION SECURITY AND PRIVACY PROTECTION

7.1 Introduction

The ISO/IEC 27002 standard includes 114 controls! Recognising the complexity and costly implementation for SMEs, this section introduces and recommends the implementation of 16 controls[7] to ensure minimum effective protection of enterprise's data. They address different levels of protection and are categorised as following:

Category	Control
Personal	**Control #13**[8]: Information security awareness
Organisational	**Control #1**: Asset management (incl. Classification procedure) **Control #2**: Policies, standards, and guidelines **Control #3**: Incident management **Control #14**: Information security aspects in relation with suppliers **Control #15**: Information security organisation **Control #16**: Additional privacy controls
Partially Organisational / Technical	**Control #4**: Access control management
Technical (ICT related)	**Control #5**: Network security and data exchange **Control #6**: Vulnerability management **Control #7**: Fighting malware **Control #8**: Backups management **Control #9**: Safeguards management **Control #10**: ICT Readiness for Business Continuity **Control #11**: Remote working **Control #12**: Cyberthreats watch

Personal category aims to ensure awareness on information security among SME's staff. The control aims to establish guidelines for SMEs' staff and users, by which they adhere to information security objectives through awareness, training, and education.

7 Some of the 16 controls in ISO/IEC 27002 consist of several interrelated controls.

8 Control number refer to the control presented in section 7.2.

The organisational category targets the management side of information security using the RACI matrix. Organising its information security, an SME has to define and allocate the essential security roles to the responsible staff with defined mechanisms for reporting to management. In addition, an SME should:

- manage and protect its digital assets,
- adequately respond to incidents compromising its data,
- develop policies and guidelines to ensure and maintain compliance regarding management of information,
- share relevant and trustworthy information with their suppliers and ensure adequate management and protection of the shared data by suppliers with sufficient response mechanisms for incidents,
- control #16 describes the additional controls defined in ISO/IEC 27701 that addresses exclusively privacy protection that has been considered important for SMEs.

Access to information entails both managerial and technical skills to maintain continuous access to data by authorised people. The access control management deals with these issues.

Finally, **the technical (ICT related) category** addresses most of the technical work related to protecting the enterprise's network. These controls address the following issues:

- facilitating data exchanges and setting up proper procedures for data backup and remote working
- addressing and managing vulnerabilities, cyberthreats, and malware
- ensuring proper safeguards and maintain business continuity following a cyber attack

As explained in section 5, ISO/IEC 27701 extends the requirements provided by ISO/IEC 27001 and extends the controls specified in ISO/IEC 27002. This section uses the same approach: a paragraph is present for each information security control that has been selected as relevant for SMEs and, when an information security control has in ISO/IEC 27701 some additional requirement in relation to privacy, a subparagraph named "Extension to privacy" has been added to that control.

It is important to note that the 16 controls presented below are the minimum required recommendations that SMEs need to implement to be compliant with GDPR requirements.

7.2 Controls

All controls discussed below follow the same structure. Once a control is stated, it is followed by a "guidance" that shows what SMEs should do to implement the control and achieve its aim. This guidance provides the **'minimum' baseline to be implemented.** As illustrated in section 4, these controls are NOT subject to risk management.

The structure of each control consists of:

- **Control**: a clear statement of an action to be initiated and accomplished.
- **Aim**: gives, as much as possible the objective that the control intends to achieve, in a SMART[9] way.
- **Scope**: the environment the control is aiming to cover.
- **Situation**: a pragmatic view of the current situation of the control within SMEs. Some of the SMEs are, of course, much more compliant and used to good practices.
- **Guidance**: a list of explained must-do actions to achieve the control, accompanied, where relevant, with a practical procedure in an Annex.

9 SMART means: Specific & Simple, Measurable (hence, concrete), Achievable/Acceptable/Ambitious (sufficiently to motivate people to act), Realistic and Time-bound. Generally, the T is to be considered as 'CONTINUOUS' as the proposed controls are considered as a minimum baseline without which no real information security management is possible.

- **Privacy**: Some considerations linking the guidelines with the protection of personal information.

CONTROL #1: ASSET MANAGEMENT

Control

Asset management should be in place to allow proper handling of information and related assets and deciding the appropriate level of protection.

Aim

SMEs will make sure that their investments (including in security and protection) are justified.

Scope

This control concerns information, processes, media containing information, ICT equipment storing, handling, and transmitting information, and physical locations where all the previous are located. This control is a complex of seven coordinated controls that are all necessary to achieve the proposed aim.

Situation

ICT assets, furniture and consumables are managed at least simply while information is not managed. Asset managed consists of the following:

- **Asset acquisition** allows SMEs to know and record the vendor, and assets are generally bought from trusted providers. It is however scarcely the case with information: the source seems not important and is not recorded. When there is a problem with the information, there is no means to complain. If the information is essential to the SME, there is nothing that can be done.
- **Asset identification and valuation** whereas identification and valuation are frequent and indispensable in the case of physical assets, it is rarely the case with information. There is no inventory of information, of the media on which information is stored, and information does not receive a value. The latter is called « Information classification ». The value of the asset is a crucial factor in determining the consequences of a risk becoming

reality. The value also eases the decision on the strength and resistance of the protection (hence the price). Determining the value of information allows SMEs to evaluate the risk of breaches to confidentiality, integrity, and availability, and to determine what you could do (value vs cost) to counter the risk.

- **Asset storage**: Assets that are not directly used are stored and the evolution of the stock is recorded. ICT equipment is stored according to the vendor's specifications and the money is in a safe.
Information is stored in files, binders, or registries, and in the memory of computers. There is however no clear idea where the information is and its status. This means that it is possible that all users do not use the same version of the information. There is generally no safe for critical information.

- **Asset use**: Assets are used according to recommended use, and policies and rules exist. ICT assets bear a label indicating the owner and its inventory code. The information is used through business processes that control the flow and the operations made upon it. The information processes are not always formally described (even in large enterprises), which causes problems when the process is automated in a computer programme.

- **Asset maintenance**: Assets are maintained according to the vendor's recommendations. There is however little maintenance on the information. Several versions can exist, and little control is made.

- **Asset exchange** within the enterprise and with external parties is recorded. The transport happens through recognised channels and the packaging guarantees there is no damage during the transport.
Information exchanges frequently happen without proper protection, and there is generally poor control on who can put a hand on it.

- **Asset disposal**: When assets are damaged, outdated or no longer usable, they are thrown away, possibly through ecological circuits. Unfortunately, information is generally simply 'deleted', and information media are discarded without due attention to what it had contained and if it has been correctly erased.

Guidance

ISO /IEC 27002 recommends managing information as an asset.

- **Information should be acquired from trustable and reliable sources**. Information coming from the Internet should be double-checked.
For example, Personally Identifiable Information (PII) — Personal Data in GDPR — provided by employees, customers and providers are to be verified, financial and accounting data are continuously controlled and monitored. It should be the same for information that has value to the SME.

- **Information should be inventoried and classified** based on the three security criteria – Confidentiality, Integrity, Availability – according to their importance for achieving the business objectives. Annex A proposes a simple technique for classifying information and the physical assets that contain and handle information.
Classification and inventory of the information do not need to happen for each individual piece of information, except for those that are of utmost value. It is however more practical to give the same classification to each category of information (e.g., PII to comply with GDPR). Information inventory should indicate the source and the date of acquisition, as in many cases information becomes rapidly outdated. **Note:** From now on, '**protected information**' refers to information that gets the level 3 or more with the technique in Annex A).

- **Protected information should be labelled.** Computer data files can receive their label in the available fields of the 'File Properties'. Indication of confidentiality, integrity and/or availability is recommended. The labelling in the footer or the header of the document is also a good solution.
Data media should receive a label according to the confidentiality level (for example by using a colour code) to indicate to personnel how they should handle them.

- Information should be stored according to their classification label whatever their support medium or their format, with specific additional rules for protected information.
    - Safeguards and backups should exist for information and applications commensurate to the value of the information (just like financial values), e.g., number, frequency, and location;
    - Measures should be in place to ensure the preservation of information integrity, whatever the duration of the storage; Protected information should undergo regular tests to verify they are readable and usable when retrieved;
    - Access controls should be in place to ensure only authorised people and applications have access under specified conditions (see Control #4).

- The Information below the 'protected' level should be handled and used with standard care. Protected information should only be used by authorised personnel and according to specific rules stated in the policies (see Control #2) as any misuse, even accidental, may put the enterprise in danger.

- Protected information should follow a formal maintenance process to ensure they remain relevant, exact, and available.

- Information exchange and communication are essential to the achievement of the business objectives. Rules should however be in place and documented to ensure that protected information is only exchanged with authorised internal and external interested parties and within an adequate container (e.g., sealed with inventory contained, encrypted, VPN, etc.). Communication of protected information to external parties:
    - should be forbidden during informal discussions and in public places;
    - during formal discussions, meetings, and conferences it should be done according to specific rules and with the formal authorisation of the enterprise top management.

- In the case information becomes useless or no longer relevant for the enterprise, it does not mean that the former has lost its value for other (unauthorised) parties:
    - as a matter of fact, they could discover something they could use to their own advantage and possibly against you;
    - plus, discarded digital memories (USB sticks, hard disks, etc.) could contain software and applications for which you have paid the license, and subsequent unlawful use by third parties can cause you legal problems.

    Discarding information should be done with care and the standard rule is that it should be erased or destroyed. Protected information should be shredded (paper, bank cards, CD/DVD), duly erased or encrypted (digital data).

Extension to privacy

Privacy is a special category of information that requires a different classification process, which is provided by a Privacy Impact Assessment (PIA) that measures the impact of security breaches on the Data Subject.

CONTROL #2: POLICIES, STANDARDS, AND GUIDELINES

Control

Documented information should exist to declare and publish the information security goals, guidelines, requirements, and guidelines to all interested parties.

Aim

SMEs will ensure knowledge and adherence of personnel and all people involved with the handling of the enterprise's information. By doing this, the SME should be and remain compliant with external and legal requirements related to information.

Scope

This control concerns all objectives, rules and recommendations that involved internal and relevant external parties need to follow and comply with.

Situation

SMEs scarcely document their objectives, rules and expectations regarding information management and security, while they do it for human resources and finances. Though, based on Control #1, information has a very important value that needs to be protected.

Guidance

Information security objectives, rules and directives should be documented and communicated to all personnel to make sure they are fixed, known, and applied.

Two important policies should be available:

- the overall information security policy that sets out the objectives to be reached on a continuous basis and that contains these deemed to comply with the GDPR (Privacy protection policy);
- the confidentiality policy that states, for persons you collect and handle the personal information (personnel, clients/customers, providers, partners), what information you need, with whom you share it and for what reason, how long you keep it, how they can use their

rights and how to introduce a complaint when they feel things are going wrong.

Specific rules regarding information storage, handling, access control, destruction, backups, communication to external parties could also be documented:

- a **standard** is a rule that must be applied in any circumstances and that can be referred to in case of non-application;
- a **guideline** is a recommendation for the 'best way' to deal with the information and its security.

It is essential that the 'policies' are signed off by the top manager and are regularly reviewed and updated to align with the changes in operating conditions and circumstances. The recommended 'guideline' is an annual review. The 'policies' should be to the point and focused on the people they are aimed to. The size and formulation depend on your specific situation and need. Documentation is the key basis to inform, train and educate people.

Extension to privacy

A specific policy concerning privacy protection should be prepared and regularly reviewed.

CONTROL #3: INCIDENT MANAGEMENT

Control

Information security incidents should be managed.

Aim

SMEs should be prepared to adequately respond to information security incidents to ensure fast and coherent resolution of all operational, financial, legal, and business disturbances and keep the damages within predefined limits.

Scope

This control concerns all incidents that are caused by breaches of confidentiality, integrity, and availability of information. This control obviously also concerns privacy breaches.

Situation

Risk management, scarcely applied in SMEs, is not always perfect, and Zero Risk does not exist. For example, fire can occur even if all preventive measures are taken. Humans may make errors and technical failures may occur.

As information is poorly managed and protected, many events and incidents occur, without being noticed and responded to as they should be. If the direct impact is not big, business consequences happen later and can be huge without any possible link with the incident.

Guidance

Whatever you do, the measures you take and the controls you implement and manage to counter the risks, events will occur and disturb your activities. If they impact your objectives, they will become a business incident. If they impact the information security objectives, they will become information security incidents. The only ISO/IEC standard describing the concepts, principles and process of incident management is ISO/IEC 27035-1. The following guidance is a short glance at what has to be done to be able to satisfactorily respond to these incidents.

It is crucial to prepare the response to incidents with predefined and tested procedures and by training, personnel to raise events and abnormal situations and the specialised teams that will be dedicated to the response.

There are 5 phases for coherent incident management:

1. Plan and Prepare

In this phase, the enterprise decides to address the incidents to prevent them from becoming unmanageable. To do that, the following should happen:

- prepare a policy to organise and manage the incidents;
- designate a person from the top management responsible for incident management;
- list the incidents you want to address;
- document (with internal and external experts when needed) the procedure(s) you intend to adopt when the incident occurs;
- decide and install the person in charge of handling the incident and coordinating the actions (incident handler);
- determine the criteria and procedure to declare an incident;
- decide and install the team that will respond to the incident according to the procedure;
- determine and install the means necessary to allow the incident handler to be informed, along with the type of information to be forwarded. These can be automated or man-activated;
- prepare and implement an awareness and a training plan to make sure all actors know what to do.

2. Detect

Make sure all personnel has the capacity of raising the event to the incident handler without risking a penalty (we all do it in case of fire or injuries to people). This should happen without undue delay, as a delay in the response could result in a disaster.

3. Evaluate and Decide

The incident handler follows the procedure to evaluate the event and declare it an incident.

- If it is not an incident, the incident handler informs the person responsible for the process, asset or ICT services of the situation allowing them to look for a correction;
- If it is an incident, the incident handler activates the response team that has the skills and capacity to act (internal or external).

4. Respond

The incident handler remains responsible for the coordination of actions until the incident is declared closed. They record the actions taken along the timeline. The response team communicates regularly with the incident handlers to keep them informed of the evolution:

- If the situation worsens or needs supplementary resources, the incident handler calls them, after authorisation from the top management when needed;
- If the situation appears to be getting out of control, the incident handler calls the top management, and the Business Continuity Plan is activated (in part or completely).

The incident handler declared the incident closed after discussion and with the approval of the affected business team.

Once the incident is closed, the incident handler completes the incident report using the predefined template and forwards it to top management.

When supplementary post-incident actions need to be done (e.g., forensics) the incident handler keeps the teams informed on the evolution.

5. Learn lessons

Each event or incident and the way the response flowed give essential information on the capability to prevent and deal with them in the future. This is the source of the Lessons Learned. A team (possibly the one that prepared the management or response plan) will gather and see what can be improved:

- better prevention of the event (improvement of the controls or operational procedures);
- better response capability (resources, skills, equipment support);
- better reporting and communication.

6. Additional information

In some cases, GDPR requires that the concerned person/people or the Data Protection Authority – the 'external party' - are informed. Business rules should also make sure that the 'owner of an information (that the enterprise has been granted access to)' is informed if something happens to it. Similarly, when someone can be impacted by an error, a bug, or an incident, they should be informed to be able to react adequately. In some cases, the 'external party' can also help the enterprise to solve the problem.

To make this possible, a communication plan should be documented indicating who is allowed to communicate outside the enterprise and how. Bad or improper communication can have serious impacts on the enterprise's reputation.

Extension to privacy

Incidents related to personal data follow the generic process for an information security incident. GDPR requires that, depending on the impact on the Data Subject, the Data Subject should be informed along with the national Data Protection Authority, within a 72-hour delay.

CONTROL #4: ACCESS CONTROL MANAGEMENT

Control

Access control should be fully and continuously managed across all its components and based on role to achieve business objectives.

Aim

SMEs will master access to information whatever they are, wherever they are and at all times.

Scope

This control is a compound of several interrelated controls which need to be defined and implemented simultaneously to achieve the objectives. This control concerns access to information (digital or on physical media) and operational facilities such as offices and ICT equipment.

Situation

Too frequently, access control resides on PCs and consists of an identifier (ID) and a password (generally weak and identical for all uses). Once the user is 'inside', they have all rights.

Correct access management is based on six elements:

1. Identity management: all authorised users are identified in a standard way. Management is however not always up to date as dormant accounts are generally not supervised and accounts of ex-users/employees are not closed sufficiently fast, leaving these accessible for uncontrolled accesses.

2. Rights management: depending on the roles covered, the rights allocated allow to access information, but also to rule activities, as well as time slots) and places from which activities are allowed.
Many SMEs, however, generally grant access without the right management. It means that everyone has access to everything or access information from a remote location, without the enterprise being able to intervene or know who did wrong in case of a problem.

3. Authentication management: all identified users use dedicated credentials to access assets and information, depending on their classification level.
Most of the time, the only authenticator is a password – generally weak – that is scarcely changed… and valid on all accounts and services. This means that once caught by a rogue employee or a miscreant, they have access to the enterprise's information with all rights.

4. Access control: accesses are only given if the identity, the authenticator, and the rights correspond.
This is generally more or less fine.

5. Event record: all accesses and attempts are logged with Date-Time Group (DTG) details, according to the classification level. Abnormalities are raised to the access controller/manager. Generally, the size of the log file is too small and, once the size is exceeded, the system starts to write on the oldest ones, mostly only a few days before. SMEs lose, by this, a lot of extremely important information needed in case of an incident.

6. Analysis of logs: logs are analysed regularly, and abnormal behaviours are identified and countered.
However, most SMEs scarcely analyse the logs, losing track of events that can indicate at least an attempt of intrusion.

If access control is applied, even partially, on ICT systems and buildings, unauthorised people can get access to protected information without much control. Its application on offices and rooms is, however, more episodic. Employees are generally not granted access to the offices (they have no keys) outside business hours. Also, cleaning of offices occurs generally outside the working hours, and the cleaning teams have access to all rooms, where information is not always hidden.

The general rules concerning access and use of money is a good example to be applied to information.

Guidance

The general – and basic – rules that follow should be applied both on ICT systems and physical locations on a continuous basis. The general idea is that users' (including applications) access to information, applications, services, and rooms are granted to what is strictly needed to perform the job that has been decided.

- **Identity management**
  - all internal and external users are registered in a standard way;
  - dormant accounts concerning users that are temporarily inactive are frozen (rights blocked, authentication and especially monitored);
  - all personnel and users that have left the enterprise have their account disconnected to avoid illicit use and are cancelled after a period that does not exceed three months.
- **Rights management**
  - rights to information concern Read, Write, Modify, Copy, Transmit/Communicate (e.g., by email), Print.
    Rights to assets concern Use, Maintain, Modify, Move (inside and/or outside the business facilities);
  - access rights are allowed to perform the activities in direct relation with the role in the enterprise and the need to access and use the information. Relation with information classification (see Annex A) is regularly verified;
  - special roles such as System Administrators, HR managers, Access analysts are linked with special rights (Monitor, etc.);
  - access rights also contain authorised time frame and authorised location (internal and/or external to the enterprise);
  - rights are regularly reviewed and adapted according to the changing roles in the enterprise.
- **Authentication management**
  - there are three authentication means used to verify the identity of authorised users: something you know (password, pin code…), something you possess (a card, a key…) and something you are (fingerprints, signature dynamics);
  - the selection of the authentication means is based on the tables in Annex A;
  - passwords and pin codes are regularly changed, especially when the authorised user leaves the enterprise;
  - the password has a minimum length of eight characters (upper and lower case, figures, and special characters) and will not be guessable by other users.

authenticator and fit the authorised time frame and origin for access;

- in case of denied access, the message indicates, 'not matching credentials';
- a maximum of attempts is defined after which the account will be frozen for a predefined period.

- **Event record**
  - all access attempts to information are recorded with the DTG and source of access request;
  - a file contains all the records for a dedicated period (at least one week for authorised accesses and two weeks for refused accesses) to allow analysis.
- **Analysis of logs**
  - analysis of logs is associated with a privileged role with a special account;
  - alarms will be raised, through the incident management channels, when the analysis shows alleged illicit attempts and when a predefined pattern is discovered;
  - dubious logs will be safeguarded (stored in Read-only mode[10]) in a way that they (1) cannot be lost, (2) cannot be modified, and (3) can serve as evidence in case of claim or judicial suits.

Extension to Privacy

Access and use of personal data require a throughout access control that follows the rules set out in the Guidance, here above.

10 The 'Read Only' (ROM: Read Only Memory) is a protection against further modifications.

CONTROL #5: NETWORK SECURITY AND DATA EXCHANGES

Control

SMEs should manage and control their networks to protect the information in systems and applications over all methods of connectivity.

Aim

To ensure the protection of information in networks and its supporting information processing facilities.

Scope

This control applies to the security management of all physical and logical devices that are part of the network and communications infrastructure, from the end-point devices to the connection to the internet. It includes mobile devices (e.g., laptops), personal devices (e.g., smartphones), Wi-Fi and connected objects (e.g., security cameras).

Situation

Basically, there are two types of networks: Local Area Network (LAN) and Wide Area Network (WAN). The LAN is the network controlled by the organisation, and the WAN is controlled by forces external to our organisation. The most famous of the WAN networks is the Internet. The separation between LAN and WAN is known as the perimeter.

Before the advent of the Internet and mobiles, the perimeter was a sturdy wall, difficult for cybercriminals to break through.

However, now the perimeter is somewhat fuzzy. Laptops, smartphones, and other removable devices constantly leave the perimeter, establishing connections outside of the organisation's control. At the same time, the information transfer between the LAN and the WAN is continuous.

Guidance

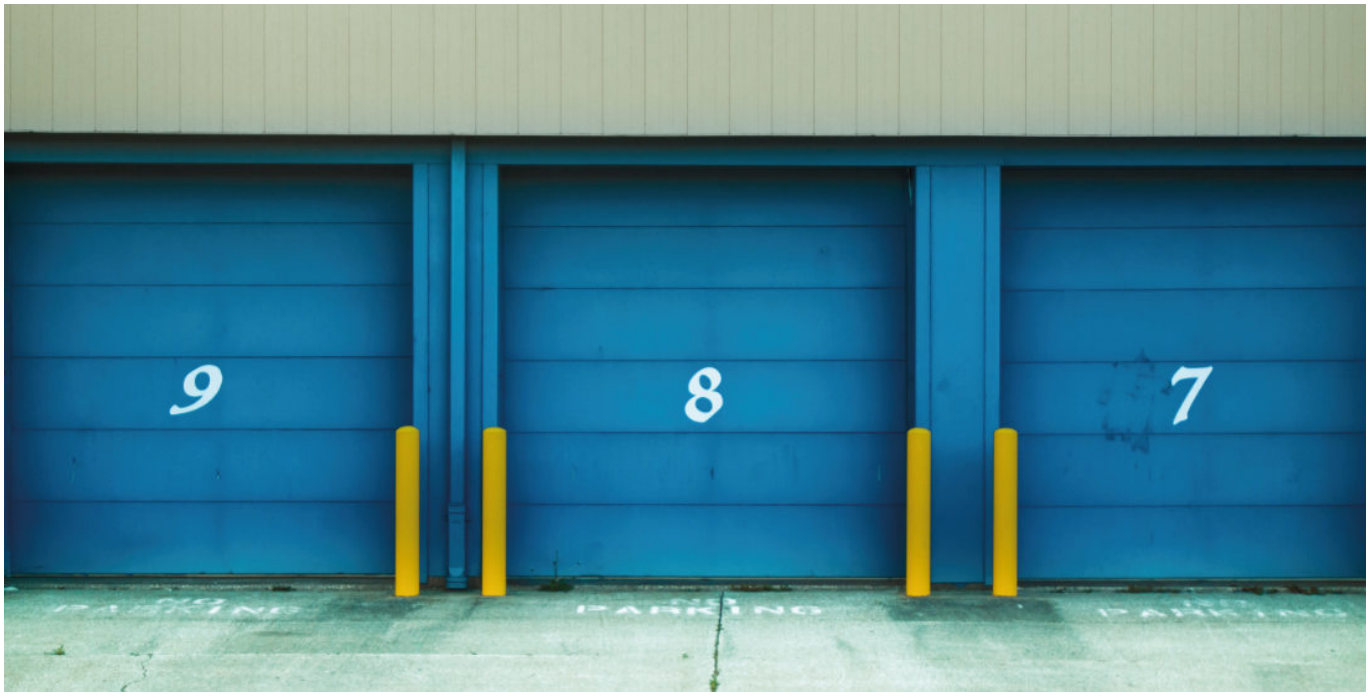
Next, we are going to highlight the most important steps to implement an adequate level of security for the network of our organisations:

- **Establish and maintain a policy for the security of connectivity**. This policy will take into consideration the rest of the points that we will see below.
- **Responsibilities and procedures** for the management of networking equipment should be established.
- **Network segregation**. It is necessary to divide the local area network (LAN) into separate networks domains, depending on the access needs of the users, and apply the rule of least privilege. Users in the finance area, for example, have no need to access information from the R&D area. If the company has a production area, it must be segregated from the management area. The segregation can be physical or virtual. Connections between network domains can be allowed, but should be controlled using a gateway (firewall, filtering router, etc.). Therefore, the network should be segmented as much as possible. It is complex, but very important, **to achieve a balance** between proper segregation of the network and optimisation of the organisation's operations.
- The policy should determine whether the organisation allows personal devices used for professional activities, known as BYOD (**Bring Your Own Device**), to connect to the network. These devices are very dangerous because they mix personal and professional issues, and because they do not have the minimum-security measures in place. If allowed, the user must agree to apply certain policies and security measures on their device.

- An architecture should exist showing the interconnection of the different **functions of the devices** in the network and their position regarding the firewall (the protected gateway to the internet).
- Implement **network filtering** mechanisms, such as firewalls or intrusion detection software; and enforce firewall policies to control inbound and outbound traffic. Apply the “deny by default” rule.
- An infrastructure drawing should exist indicating the internal IP addresses, the Operating System (OS) and the type of data hosted.
- **Restrict physical and logical access** to network devices. All systems on the networks should be authenticated, and systems connected to the network should be restricted. In addition, the impossibility of physical manipulation of network devices must be ensured.
- A user outside the perimeter should not connect to **WI-FI connections** that are not under their control or under the control of their organisation, as they are especially insecure. It is much safer to connect via mobile phone.
- The Covid-19 pandemic has greatly increased **teleworking**. This means connecting to our local network (LAN) through a public network such as the Internet (WAN), in order to work. Use a Virtual Private Network (**VPN**), with IPSec encryption, if possible, for teleworker connections. During the pandemic, many companies, especially SMEs, have lowered their security requirements to allow teleworking, which has caused a greater number of security incidents.
- **Logging and monitoring** should be applied to enable recording and detection of actions that may affect, or are relevant to, information security.
- Carry out periodic **penetration testing** to determine the adequacy of network protection.

Extension to privacy

Much of the information that travels through the networks (LAN and WAN) can be classified as personal data. Therefore, special controls[11] must be in place to ensure the integrity and confidentiality of this information. The most common measure is the encryption of communications, avoiding "man in the middle" attacks, which consists of intrusion at any point of the communication line between the sender and the receiver, capturing the network frames through the information travels.



11 See Annex A of the SBS SME Guide for the implementation of ISO/IEC 27001 on Information Security Management, p.30: 10.1.1. and 10.1.2

CONTROL #6: VULNERABILITY MANAGEMENT

Control

SMEs should minimise the risks resulting from the malicious exploitation of known vulnerabilities. It is, therefore, crucial to implement safeguards to remove or control the vulnerabilities, maintain a list of remaining known vulnerabilities, and raise awareness of these vulnerabilities within the SME.

Aim

SMEs minimise the presence of vulnerabilities and enable the security-cautious behaviour of their staff.

Scope

Based on the SME's current and complete inventory, the SME checks for each asset for patching or applying other protection mechanisms. Priority should be given to assets that are critical for the SME's business or exposed to important and new threats (see Cyber Threats Watch). This includes OS.

Situation

New vulnerabilities are discovered continuously for any type of digital asset. Vendors are releasing patches and publishing recommendations for vulnerabilities that get known for their products. Many SMEs do not this into account and are, for example, still working with outdated OS and applications that are no longer maintained, due to financial or operational constraints.

Guidance

Vulnerabilities should be addressed at least once per month and when incidents have been experienced by the SME. Vulnerability management may be performed by a designated person who assists the asset users in the checking and removal or control of the vulnerabilities.

Vulnerability management is a multi-step process with one preliminary step and three steps that will need to be repeated regularly (at least once per month) or upon an incident that is experienced by the SME.

1. **Identification of digital assets**: The SME must create an inventory of digital assets (section 7.1) and, for each asset, determine how the vendor releases patches or publishes recommendations.

2. **Prioritise assets for vulnerability assessment**: The SME should prioritise the inventory of assets for business criticality of the asset and exposure of the asset to new or critical threats (see control Cyber Threat Watching).

3. **Patch assets or apply other protection mechanisms**: Each asset should be checked for the presence of new patches or recommendations. These patches should be checked for whether they imply risks or costs that the SME cannot bear and tested before they are installed on all assets of the same type. Acceptable patches must be installed. For trusted vendors and when backups of the concerned assets are available, patching may be automated. Assets that cannot be patched should be protected with alternative means, turned off, shielded by access controls like firewalls, or monitored closely.

4. **Communicate remaining vulnerabilities**: The SME must track the patching progress in the inventory of digital assets. It must inform the staff about unpatched assets and offer recommendations for safe or cautious interaction of the users with these assets.

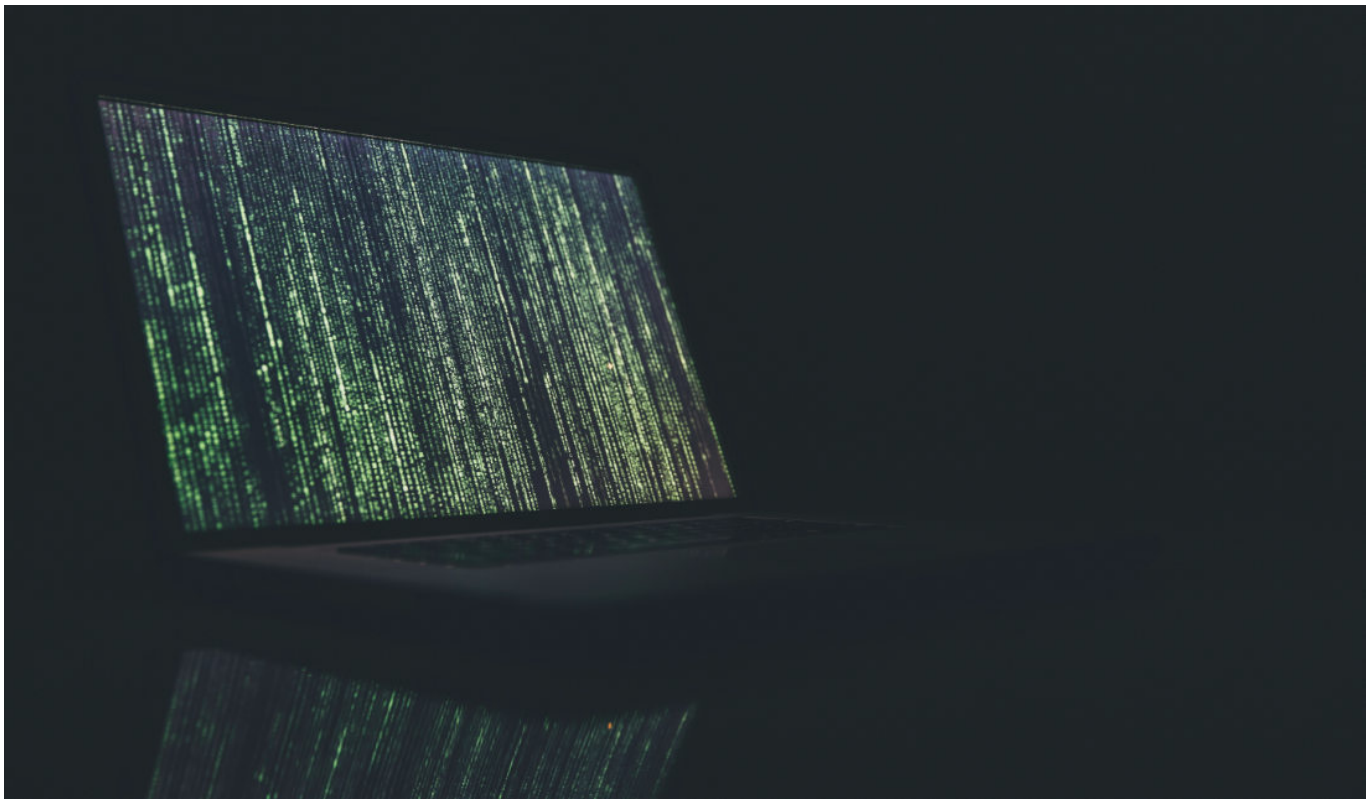
5. **Periodically implement patches and recommendations**: Patches and recommendations should be implemented by the SME as rapidly as possible if the protection benefit outweighs the risks implied by closing the vulnerability.

Although these patches and recommendations should be implemented by the SME as rapidly as possible if the protection benefit outweighs the risks implied by closing the vulnerability, SMEs rarely implement those patches.

The SMEs are recommended to share their experiences with patching with other SMEs. Within such a community of practice, SMEs can benefit from each other for improving the efficiency and effectiveness of their vulnerability management and share advice concerning problematic assets or patches.

Extension to privacy

When assessing vulnerabilities, the SME should prioritise assets used for managing information depicting customers and users.



CONTROL #7: FIGHTING MALWARE

Control

SMEs should implement and maintain a policy and appropriate tools to counter malware.

Aim

To stay protected against the damages malware can cause to ICT systems, business processes and objectives.

Scope

Malwares are much more complex than SMEs and individuals think. These malwares spread into the computer system through:

- an infected file or contact;
- a phishing email;
- the agency/action of a hacker;

- visiting an infected (or malevolent) website.

Whatever the type or and way of infection, the effects range from benign to extremely grave.

Situation

In the same way, as individuals do, SMEs scarcely pay any attention to the vast range of malware infection modes and consider the acquisition and regular update[12] of an "antivirus" software sufficient. Most of the time they keep the same solution for decades.

Guidance

SMEs should:

- regularly review their anti-malware policy to keep it up to date with the threat environment and the business/technological context; this means verifying with experts and reliable sites the best solutions as the effectiveness varies along the time;
- make sure all computers are continuously protected;
- install on computers, servers, and communication nodes different technologies of anti-malware solutions – to allow cross-detection capabilities;
- verify that their security awareness program regularly come back on the anti-phishing drill so that employees and users will not fall for the hacker's tricks;
- regularly analyse the cyber threat situation using public/private reports (<sources>) or by consulting a specialised body and review their preparation.

Extension to privacy

[No specific issues related to privacy protection]

CONTROL #8: BACKUP MANAGEMENT

Control

Backup copies of information, software, and system images should be taken and tested regularly in accordance with an agreed backup policy.

Aim

Information is the most valuable asset of a company. Therefore, it is necessary to have copies that ensure their availability, integrity, and confidentiality.

Scope

This control applies to all information, software, and systems configurations of the organisation.

Situation

Different risks threaten the information held by organisations (ransomware and other attacks by cybercriminals, hardware or software failures, human errors, fires, or floods, etc.). However, on many occasions we keep finding a lack of backup copies, or copies made in a poor way, from which it is impossible to recover their content.

In addition, to force the payment for recovering the information, cybercriminals try to eliminate the backup copies before proceeding to encrypt the information using ransomware. Thus, it is becoming essential to have an off-site copy.

12 The European Expert Group of IT-Security provides updated information on antivirus solutions. In addition, most anti-virus or security solutions provide a list of the latest malware/spyware/trojans.

Guidance

A backup policy should be developed to establish the organisation's requirements for backup of information, software, and configurations. Also, retention policy and backup protection requirements must be defined for each type of information.

For the backup procedure, we recommend using the 3-2-1 Backup Strategy:

- (3) Maintain at least 3 copies of your data.
- (2) Keep 2 copies stored at separate locations.
- (1) Store at least 1 copy at an off-site location.

One copy is the production data, the other two copies are backups. Each of these copies should contain the same version of the data, from the same point of time. At least one of the copies must be in a different location, at a sufficient distance to be safe from a disaster at the main site.

Backup information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site (please refer to Control #9: Safeguards Management, below). All backups must be encrypted. Access to backup software and storage must be protected with specific administration credentials.

The backup logs should be reviewed daily to check if the copies have been completed correctly, or if errors have occurred.

Not all information in an organisation is equally important to the business[13]. For this reason, backup plans must be designed to optimise the process based on information security requirements.

Depending on the type of information, the existence of different retention policies is one of the most complex points when designing backup plans. Since the retention policies also apply to the information stored in backups, it is usually necessary to configure different backup plans depending on the different retention periods.

Finally, restoration tests should be carried out periodically on the backups made to ensure that the information can be restored when necessary.

Extension to privacy

In most cases, backup copies contain personal data, so it is especially important that the copies are stored encrypted, and that the retention periods[14] established to comply with the GDPR are met.

CONTROL #9: SAFEGUARDS MANAGEMENT

Control

SMEs should protect important information and digital assets from loss, destruction, and falsification.

13 Cost considerations also play a role here. For example, the enterprise must copy ERP database changes every day, but the photos of the last congress once a year. If the enterprise has a copy in cloud storage it could be an important cost.

14 Retention periods depends on sectors, applicable laws, type of information, customer contracts and other factors. There are no defined rules for all.

The protection includes the planning, creation, and repeated testing. A particular safeguard is backups[15].

Aim

SMEs should protect important information and digital assets from loss, destruction, and falsification.

Scope

Based on its inventory of digital assets, the SME plans, creates, and repeatedly tests safeguards. Safeguards for protecting hardware include the use of locked rooms or cabinets and the use of anti-theft systems. Safeguards for protecting software and information include authorisation, e.g., with strong passwords and second-factor authentication, encryption of storage and transmission of data, e.g., with a VPN system, and protecting digital assets with anti-malware, firewalls, and system logging. Staff managing the safeguards and staff with access to secret or personal information should be checked for trustworthiness. Backups should be created at regular intervals and their recovery tested.

Situation

Many types of attacks target unauthorised access, eavesdropping, falsification, and theft of information. In addition, digital assets may break or become unusable due to a diversity of reasons. Safeguards are established to protect against such types of threats.

Guidance

Safeguards management is a multi-step process with one preparatory step, four protection-oriented steps that will need to be repeated regularly (at least once per month), and one security culture-building step to be repeated for each new staff and at least once per year.

1. Identification of digital assets: The SME must create an inventory of digital assets (section 7.1) and, for each asset, determine its business criticality. The SME should prioritise the inventory of assets for business criticality of the asset and exposure of the asset to new or critical threats (see control Cyber Threat Watching).

2. Protect access to digital assets: The SME should determine how each of the digital assets shall be protected, including physical safeguards for hardware, digital safeguards for software (e.g., with access control with strong passwords or two-factor authentication, endpoint protection with anti-malware), network (e.g., with encryption and firewalls), and data (e.g., encrypted storage and transmission and by using a VPN).

3. Protect against loss of information and software: The SME should create an up-to-date backup of systems and of information critical for the business. The backups should be versioned, and the ability to recover the systems and information tested.

4. Plan threat-specific safeguards: For each new or critical threat, the SME should consult the recommendations for preventing and defending against attacks. CERTs providing threat information commonly offer such recommendations.

5. Establish trust: The SME should check technical staff and staff with access to critical information for trustworthiness.

6. Establish a strong security culture: The SME should instruct all staff about safe or cautious behaviour, including how to work with backups, how to use business - critical assets, how to protect access to assets (e.g., by using unique and strong passwords or two-factor authentication), and how to work with backups and recovery. A strong security culture also includes training of staff to detect attacks, e.g., based on diverse forms of phishing and social engineering.

Extension to privacy

15 Refer to Control #8: Backup Management.

The GDPR requires the SME to ensure appropriate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage. The SME must designate a person, the "controller" who is responsible for the protection and demonstrate compliance.

CONTROL #10: ICT READINESS FOR BUSINESS CONTINUITY

Control

ICT systems should be designed (Security by Design and by Default) and built to resist and be resilient to failures and problems.

Aim

SMEs are confident that ICT failures and problems have no serious detrimental effect on the business processes, objectives, and stakes.

Scope

This control covers ICT systems and physical facilities that allow them to operate (e.g., power, air conditioning, a roof, and skilled people).

Situation

Whatever the cause, unexpected situations test the competitiveness and capability of a company. If a business handles crises effectively, its market value and reputation can thrive. So, it is crucial for a company to be ready for business continuity especially from an ICT point of view.

A Business Continuity Plan (BCP) helps make companies as resilient as possible because it can:

- limit interruptions (the less downtime, the less money lost); lay out alternatives (to quickly

restart business operations);

- empower employees.

Guidance

Every company rarely gets advance notice that a cyber-attack is ready to strike, and no one thinks that each incident is unique and unfolds in unexpected ways.

If an entrepreneur or a top manager wants to give their organisation the best shot at success during a disaster, they need to put a current, tested plan in the hands of all personnel responsible for carrying out any part of that plan; however, before talking about plans, actions and remediations, it is important to focus on the three main pillars and five principles for business continuity.

The three pillars are: company culture/awareness; policies; technology.

Company culture/awareness

Embracing awareness is fundamental to integrating business continuity practice into business and changing the organisation's culture is the most difficult thing to do because it needs a lot of time to be implemented.

In general, here are the steps that any organisation should use to increase its business continuity culture:

1. Start from top management. Engaging with top management may sometimes be hard. However, it is key because business continuity change occurs through a top-down approach. Start by introducing business continuity concepts and showing long-term benefits, especially from a financial point of view.
2. Build a team of influencers who understand benefits and help to build company resilience.
3. Always use a collaborative approach to get all employees to try to improve or change your company culture.
4. Invest in training, including webinars, white papers, informative materials. We recommend repeating simulations three times in a year and remember that business continuity is not a single picture but a never-ending film!

Policies

Business continuity policies are created to enforce company organisation, following market and compliance requirements. They document what is needed to keep an organisation running on ordinary business days as well as during an incident. When policies are well-defined and clearly adhered to, the organisation can set realistic expectations for business continuity and processes. Policies are also used to measure what went wrong during a crisis, to improve the company's resilience and to address problems.

One of the primary things to consider when crafting a business continuity policy is the particular risks an organisation is likely to face. Referring to ICT readiness, the first question to ask is: have there been problems with IT incidents in the past that need particular attention? Accounting all these factors could help to create good policies.

The backbone of BC continuity policies is Business Impact Analysis and Risks Assessment.

A Business Impact Analysis establishes the effects of a potential disaster on an organisation by finding existing vulnerabilities and focuses mainly on the business impacts, recovery time, and recovery point objectives.

The other reliable method to discover potential threats is to determine their likelihood with a risk

assessment to identify hazards and to find ways to reduce their impact on business and promptly reduce time to establish the new normal after an incident. A risk assessment should help to:

- identify hazards;
- evaluate risks;
- create control measures;
- record the findings;
- monitor improvements.

Technology

Once an organisation has developed its culture and its policies, it is time to think about technologies that can help to build better resilience.

Even if organisations have modest cybersecurity budgets, they pay attention to their resource consumption as these resources have a great chance of being targeted by cybercrime. Thus, to build BC readiness we must start on securing two important assets:

- Users
- Environment

Business Continuity Plan

The main purpose of a Business Continuity Plan is to retain human resources, protect assets and keep the business running as much as possible during an emergency so that normal operations can be resumed as soon as possible.

Based on the assessment, preparedness, response and recovery, a Business Continuity Plan will ensure:

- people commitment
- quality
- growth

- customer satisfaction

Why does an organisation need a BCP?

"It won't happen to us" is the easiest thing to say and think about when a disaster does not seem to be on the horizon. However, disasters have no boundaries and whether a crisis is happening or not, it is a good idea to be prepared with a plan to help your business to react. Be ready for the unknown and remember: if you can manage a problem, you will be able to tackle the issue and assess what is going on and when you will go back to normal.

When an IT incident happens, customers, employees and partners need to know that they are protected and will be looked after. The BCP will cover everything within the business and build your company reputation.

How to make a Business Continuity Plan

First of all, remember that a BCP must concentrate on these three key factors:

- Resilience
- Recovery
- Contingency

So, what should a Business Continuity Plan include? The right answer is it depends on the disaster.

In a perfect world, you should have tailored plans for each potential issue. How you deal with a network issue is not going to be the same as how you react to a pandemic crisis and the recovery process will not be the same either.

1. **Identify risks**

Start asking yourself questions like:

- How will staff get to the office?
- If they cannot get there, will they work remotely?
- Do you need to get hardware sent to them so they can work from home?
- Where will you place staff who can get into the office?
- How will you communicate to staff, board members and customers about the disaster/ damages?
- Will you need to replace anything following this disaster?
- Do you have the budget to be able to replace things and potentially set up another office?

These questions will give you a very basic idea of how your business might be affected and how you will have to respond to this disruption.

2. **Decide what you need to protect**

Identify what you need to protect and where you might be the most vulnerable.

Think about information that might be inside the office and think how to protect them even if they are not digital. Think about people, do not forget that they help to keep the business going.

Consider how they will continue to work.

Take a look at processes and policies. You need to protect your operations and services for the sake of the company and for the clients that use them.

3. **Identify measures to manage risks**

Assess what measures you currently have in place and what might be missing.

4. **Create your plan(s)**

Consider in greater detail about how you are going to organise the staff, protect the office and ensure the business as a whole will be fine during this period. These plans cover security, safety, and general plans to protect the business.

5. **Practise and practise again!**

Do not leave your plan in a drawer. We recommend planning some form of testing twice a year.

Experience is valuable. Use your worst scenario and transform them in best practices.

Practising will give you the opportunity to see how effective your plan might be. This is especially helpful if you are missing something or if something really is not going to work and needs to be planned in a better way. Ask for feedback from employees, customers, and suppliers.

Why companies need a Business Impact Analysis (BIA)?

A BIA helps you to identify and document critical business processes and their supporting elements. This aids in understanding your environment, and what is most important, before you take steps to protect it. BIA reveals how those keystone operations and functions would impact business continuity if they were hindered or eliminated.

What does BIA achieve?

- Identify key business processes and functions.
- Develop priorities, business processes and functions.
- Establish a detailed list of requirements for business recovery.
- Figure out the impact on daily operations.
- Develop recovery time requirements.
- Determine the financial, operational, and legal impact of disruption.

How to conduct a Business Impact Analysis (BIA)?

- The first step in performing a successful BIA is to ensure that the right business activities and resources are in-scope. Once products and services are identified as in-scope, required

departments should be identified for inclusion in the BIA process.

- After identifying in-scope departments and activities, schedule meetings with each department's leadership. For a better result, all participants should:
  - know the organisation's key priorities (as they relate to products and services);
  - understand the day-to-day activities assigned to the department;
  - understand the resource dependencies required to complete each business activity.
- Execute BIA and Risk Assessment Interviews to determine the activities the department performs that supports the delivery of in-scope products and services. For each activity, it is important to fix all the steps necessary to complete the activity, peak operation times, downtime impacts (i.e., financial, reputational, operational) and the dependencies required to perform each activity. We suggest documenting the following dependency types:
  - Applications
  - Facilities
  - Third-party suppliers
  - Equipment
  - Personnel
- Document and approve each department BIA report with the meeting results. These reports should contain all information and recommendations collected during each interview.
- Complete a BIA Summary for management's review and approval. The purpose of this task is to provide an overview of the key activities, resource requirements, and risks identified during the low-level meetings.

CONTROL #11: REMOTE WORKING

Control

A policy and supporting security measures should be implemented to protect information accessed, processed, or stored at teleworking sites.

Aim

Remote work is increasingly common and is forcing companies to establish specific security measures for an environment in which the perimeter is more and more diffuse. It will protect the enterprise against information theft and illicit intrusion in its ICT systems through the communication channels and improper use of computers that are out of their control.

Scope

This control applies every time users work from a location outside the office where they develop their activity on a regular basis.

Situation

Remote working has been growing in recent years progressively. However, because of the COVID-19

pandemic and the consequent confinement, the need to provide all workers with the necessary equipment and access rights to work from home has resulted in companies relaxing security measures to facilitate remote work.

Cybercriminals have taken advantage of the situation to deploy all kinds of mechanisms that allow them to obtain user information, hijack information, carry out targeted attacks, etc.

In the post-pandemic, teleworking will not return to the previous situation but is expected to be increasingly important in the development of business activities.

Guidance

These are the most important steps to implement an adequate level of security for remote working:

- Define, approve, and distribute a specific security policy for remote work that contemplates the proper use of corporate media and covers all possible variables, such as the use or not of domestic computers and the possibility of accessing them to verify the security of the equipment, the need for software licenses, the requirements for communication lines, the security of the workplace and the preservation of the confidentiality, etc.
- Whenever possible, the equipment to be used in remote work should be corporate computers, and the user should never use them for personal matters. Therefore, users should not use home computers for professional business.
- Users should only connect to Wi-Fi networks under their control and with WPA2 type security.
- The company must define and configure the endpoint protection for remote workers, and make sure it is active and up to date.
- Also, the OS must always be up to date.
- Corporate equipment supplied for remote work, usually laptops, must be encrypted.
- The channels for videoconferencing must be encrypted.
- Provide connectivity through a secure VPN, using IPSec protocol if possible.
- Avoid using remote desktop connections, as they are one of the main attack vectors.

- If possible, two-factor authentication should be implemented.
- The user must ensure that his work is stored in the corporate systems. A common mistake when working remotely is saving work documents locally, so they cannot be included in the backups configured by the company.
- Do not relax security measures to facilitate remote work.
- Be sure to revoke access rights and return of the equipment when the remote working is terminated.
- Train the personnel to prevent undue access to the equipment and data by safeguarding them in a closed cabinet.
- Train the personnel to ensure they avoid working on 'protected information' (see Section 7.3: Asset management) while people are walking around.

Extension to privacy

When working remotely, personal information travels through external networks until it reaches the corporate network, so it is very important to use VPN connections. In addition, in a domestic environment, special attention must be paid to the privacy of the information.

CONTROL #12: CYBERTHREATS WATCH

Control

New and emerging threats challenge SMEs to adapt their security practices to stay protected continually. It is, therefore, crucial to observe changes in the threat landscape.

Aim

SMEs are protected against new and emerging threats by deriving their need for security controls from an up-to-date understanding of the threat landscape.

Scope

Security controls are implemented based on risks resulting from threats. Consequently, risks must be assessed each time when new threats are identified. The scope of this control is threat identification for risk assessment and risk mitigation planning. The risk management will be subject to other controls.

Situation

A wide range of threats represents information security risks that can hamper your business continuity. While the broad categories of threats remained stable over the last decade, new attacks are invented and tried all the time. Also, these threats differ by geographical location and by industry.

Guidance

Cyber threat watch is a four-step process with one preliminary step and three steps that will need to be repeated regularly:

1. **Identification of sources**: The SME must identify all sources for threat information to consult when learning about new threats. These sources can include publications and reports from special interest groups, cybersecurity agencies like national CERTs, and trusted companies and media specialising in threat monitoring.
2. **Identify new threats**: When consulting a source, new threats should be documented. Threats can be marked as being not applicable/relevant if a justification for doing so is given.

3. **Determine impact on risk assessment**: Identified threads must be integrated into the risk assessment to determine if they lead to new unacceptable risks.

4. **Planning of treatment action**: If new unacceptable risks arise from the third step, appropriate action must be planned to mitigate these risks.

It is important to understand cyber threats watch as an activity to be repeated at regular intervals. For the SME, it is important to be aware and stay updated about the important threats by looking for new threats every three months.

For the identification of sources to obtain information on new threats, a yearly cycle can be used.

Also, specific attacks such as the Flubot scam may affect an SME within hours of its first appearance, calling for immediate action, e.g. a warning on the company's internal communication channels. News reports may provide early warnings and acting according to trusted recommendations will result in a timely answer.

1. **Identification of information sources**: Typical sources include special interest groups, cybersecurity agencies like national CERTs, and trusted companies and media specialising in threat monitoring. Examples:

- ENISA aggregates and publishes threat information for the whole of Europe approximately once per year. These publications offer a general, coarse-grained overview of the threat landscape.
  - Overview of publications
  - Top threats for 2020
- In each EU Member State and other European countries, official Cybersecurity Centres[16] have been established. For SMEs, they offer up-to-date local threat reports, recommendations, and subscriptions. The following points may be helpful for threats specific to the SME, especially given its location. An example of CERTs with information for SMEs[17]:
  - Romania, Directoratul National de Securitate Cibernetica
  - Switzerland, National Cybersecurity Centre (NCSC)
  - The Netherlands, Dutch Digital Trust Center

2. **Identify new threats**: New threats should be documented and be used to minimise the time needed for the risk assessment. Threats that do not apply to the SME should be included in the documentation and marked with a justification for the dismissal.

3. **Determine impact on risk assessment**: Once a new threat is identified, the SME should review its risk assessment to ensure adequate protection of the SME. One or more risks may be added for each asset to which the threat could apply. If a similar risk is already listed, its likelihood and impact must be revised.

4. **Planning of treatment action**: After risk assessment, the risk scores must be evaluated. For new risks, introducing new security controls may be appropriate to reduce the risk to an acceptable level. For risks that have been changed due to a new threat, the changed risk likelihood and impact may

16 ENISA has published a report on CERTs with recommendations on baseline capabilities
17 Annex D contains a full list of CERTs in the Member States + UK

have increased the risk score. Therefore, the SME may need to adapt its security controls. The new and adapted security controls should be prioritised and planned for implementation.

Extension to privacy

When evaluating threats during the risk assessment, the SME should consider the impact on information availability, integrity, and confidentiality. For protecting privacy, special attention should be paid to assets containing personal information and threats that could affect the confidentiality of the information contained in this asset. (see Control #1 : Asset Management)

CONTROL #13: INFORMATION SECURITY AWARENESS

Control

Personnel and users of information and ICT systems should be made aware of the information security objectives and rules. Expectations should be clear and understood. Personnel with specific roles should be trained to accomplish their duties.

Aim

SMEs are confident that their personnel and users abide by the information security objectives and behave as expected in most cases.

Scope

This control applies to all information handled by the enterprise, and on the IST systems and applications that give access to and allow handling of business and related information. This includes financial and private information.

Situation

There are four levels with regarding communicating information:

1. Informed: Regarding this, people are saying that there is something available somewhere; it is similar to the news. No one is obliged to read it and to apply it. In relation to information security, this option is not relevant and should not be chosen.

2. Aware: Using this mode of communication, personnel and users are forced to read and should become conscious of the issue, the objectives along with their role and responsibility. As many of these changes frequently - i.e., business objectives and processes, threats to information, available solutions - awareness sessions (and programs) should be repeated regularly.

3. Trained: With this mode of communication, people who have a specific role or that has to gain a new attitude, a new habit or a new competence receive all they need to do what is expected from them.

4. Educated: This is the highest model of communication where the involved personnel gain a supplement of information so that they know the whereabouts and understand why the specific objectives have been set and how the directives, procedures and mechanisms allow achieving the objectives.

In most SMEs, the security objectives are not set. In the others, people are just informed that a policy has been posted and is available. Awareness is sometimes present, at least when new personnel is hired. The knowledge is not regularly updated. Training is limited to the strict minimum and key security roles are scarcely educated.

Guidance

SMEs should list what knowledge their employees (and users) need to have to help achieve the business and related information security objectives. These concerns:

- the security policy;
- the confidentiality policy (with reference to Personal Data);
- the security processes and procedures to follow;
- the correct use of the information, ICT systems and the security mechanisms;
- the threats they may face while working;
- the reaction to have in case of anomalies and incidents (as it is done in case of fire).

The content should be fixed along with the most appropriate mode of transmission/teaching.

A plan and program should be defined and implemented to make sure all the personnel and specific roles are fully ready to perform as expected.

After each session, and after a few months, a test should be done to verify the acquired knowledge and skills. This allows the progressive adaptation of the content and the plan to the real context, and make sure the personnel apply the rules.

Extension to privacy

Privacy protection awareness and training are required by GDPR, on an annual basis.

CONTROL #14: INFORMATION SECURITY ASPECTS IN RELATIONS TO SUPPLIERS

Control

Contracts with suppliers should clearly state the organisation's expectations with regards to information security, incident management, ICT readiness for Business Continuity.

Aim

SMEs are confident that their suppliers know how to handle the information they are entrusted in relation with their classification level and their role and requirements in case of an incident and crisis.

Scope

- To ensure trustworthy agreements in relation with suppliers and outsourcers, this control concerns:
- SME's information that is necessary to carry on the signed contract;
- Expectations and requirements in provisioning/delivering the contracted assets and services;
- Expectations and requirements supporting the SME in case of incident and crisis; Rules to be followed in case of conflict during the life of the contract; End of contract clauses and rules (with relation to retrofitting or destruction of provided/stored information).

To ensure the aim is reached, the scope of this control also addresses information security requirements during the 'call for offer' phase, the preparation, signature, and maintenance/evolution of the contract expectations.

Situation

Each partner in the relation has its own risks. If an event occurs on both sides, the consequences could be hugely different. Some partners in the supply chain can experience specific threats/events that can jeopardise the whole chain.

As the supplier has to know the acquirer's risks (or at least feared threats) to counter them, they have access to key information and the misuse of which are detrimental to the acquirer.

The final customer (consumer) has also specific risks that the supply chain should identify and manage.

Risks in relation to acquisition of product (mainly but not only ICT)

- To provide the 'good' product, the supplier needs to know the acquirer's "needs" and some exchanged information that can be sensible.
- Failure of the product to comply with the specifications can impact the acquirer's capability to perform especially if it concerns critical ICT infrastructure.
- Vulnerabilities in the product can jeopardise the acquirer's security posture.
- Supplier access to the acquirer's ICT systems and information.
- The acquirer access to the supplier's ICT systems.
- The acquirer can require the monitoring of supplier's production & outsourcing processes

Risks in relation to acquisition of services

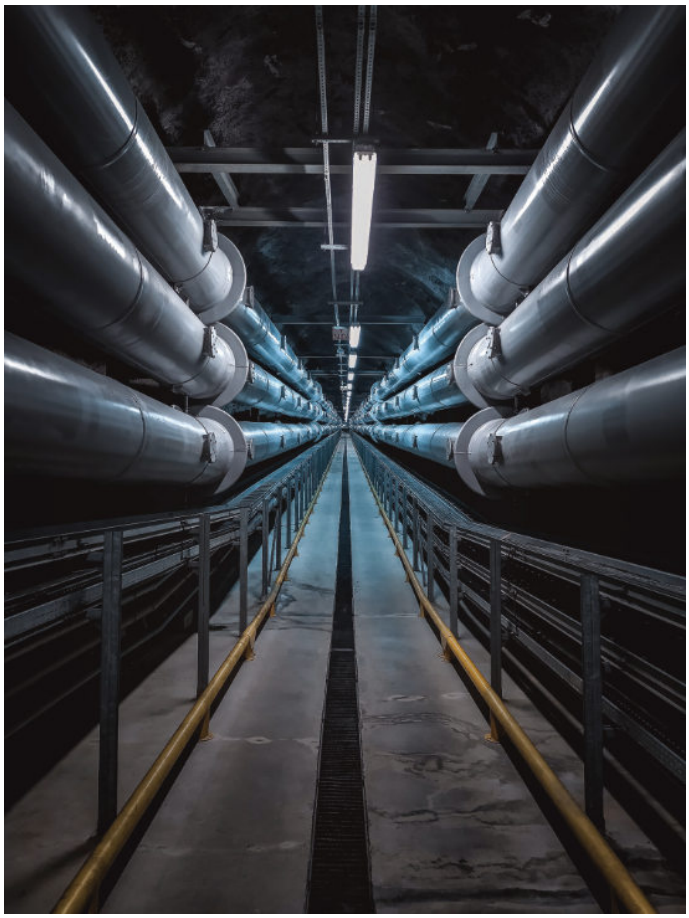
- The supplier access to the acquirer's information (outsourcing, Cloud, BU, ICT equipment maintenance, etc.)

- The supplier has access to acquirer's facilities (e.g., cleaning services as the activities very often happen outside the office hours and cleaners have access to all rooms and places).
- The acquirer can require the monitoring of supplier's processes to control quality (and security of service, e.g., GDPR)

Rules in relation with GDPR

- Rules for access, storage location and retention of acquirer's PII.
- The acquirer should ensure the supplier chain control when the supplier outsources part of his activities, that the same 'conformance rules' are implemented.

Gap



This control is scarcely implemented by SMEs, as it is also the case with bigger organisations. It is probably due to the fact that information is not managed (see control #1) and, hence, not given a proper value to show how sensitive it is. This control is particularly important with Cloud services.

Guidance

To ensure proper management of information security risks, a policy should state the rules the SME should follow when opening, signing, operating, and terminating contracts with suppliers of products and outsourcers of services. This policy will determine which control the enterprise wants to have on the services/products supply chain of the supplier.

Within SMEs, contracts should be prepared and signed by one single person from the top management.

The Contract should be based on a clear purpose as the acquirer needs to support business activities, or specific activities are beyond its competencies but essential for achieving business objectives (e.g., ICT).

The information security principle of 'Least privilege' should be kept in mind so that the supplier gets access only to information that is necessary for 'performing' the contract. Protection concerns the access to, and transfer of information on the three security criteria: Confidentiality, Integrity and Availability! This could be done through:

- Presence and activation of good practices and processes (e.g., ISMS, GDPR, etc.)
- Control of supplier access to acquirer's information & facilities
- Service Level Agreement (SLA) & reliance

A checklist

The contract should contain mutually accepted security clauses and annexes (e.g., for GDPR or product/ service in relation to business-critical activities) formulating a set of controls and responsibilities regarding

the implementation and monitoring, and rules in case of conflicting solutions to implement controls and in case of information security incidents including privacy-related incidents.

- The contract should define the information exchange protocols to be used when "protected information" is shared.
- SMEs should:
  - make their personnel aware of the rules fixed by the contract on information exchange with suppliers.
  - make their personnel aware of the use of outsourced services.
  - make their personnel aware of the use and maintenance of the acquired product.
  - determine and monitor the access control rules for suppliers on the enterprise's ICT systems.
  - determine and monitor the physical access of suppliers/outsourcers to the facilities, as it does for visitors.
- A registry of the acquired products and services should be created with the list of involved and exchanged information. This registry should be kept up to date and reviewed for any change in contract or information classification level.

Extension to privacy

When the supplier has access to, and needs to handle PII, they must comply with GDPR as a data processor. All these rules should be applied when personal information is handled by, or exchanged with a supplier/outsourcer, in the application of GDPR.

CONTROL #15: INFORMATION SECURITY ORGANISATION

Control

Essential roles related to information security should be defined, described, and allocated to sufficiently educated people who should report to top/senior management. The use of a RACI matrix is generally recommended as this tool allows to clearly delineates all responsibilities and specifies when each role intervenes.

Aim

SMEs personnel knows who is responsible for information security and the essential roles that are activated.

Scope

This control addresses all roles and responsibilities in relation to information security.

Situation

Information security roles are scarcely defined and allocated in SMEs, for the simple reason that there is no sufficient and adequately educated personnel. These roles are however important and some, especially these in relation to the GDPR, are mandatory.

Guidance

Several roles and functions are key to ensuring a coherent and continuous management of information security, both for IT and non-IT environments. Some roles can be allocated to the same person, as long as this does not create a conflict of interest and put on the same person the action and its approval. All roles should report to the top management who makes the final decision and bears the responsibility.

Most of these roles will need a 'task force' for the preparation phase as they need the knowledge and participation of all departments. These roles can be outsourced, but the contract must be clear and follow recommendations set out in control #14. The final responsibility will however always rest on the SME itself.

The organisational and personnel structure must be individually adapted to the circumstances of the company. With regard to the composition of the committees, a distinction must be made between the introduction phase and the maintenance of the project.

At the very beginning, a project manager should be designated to tackle the introduction of information security in the company and to assume the role of the information security officer (ISO).

The task is to establish, promote and coordinate the information security process. To fulfil these tasks, it is desirable that the ISO has knowledge and experience in the areas of information security and information technology. For this reason, the selection of this person often falls on employees from the information technology department. The role of the ISO can be performed in staff collaboration with the data protection officer or by another employee from the organisation. The ISO and its responsibilities must be made known to all employees. The ISO reports directly to the company management and is

entered in the organisational chart as a 'staff position'.

We recommend considering the following points when appointing the ISO. Firstly, when possible, the ISO should not be the IT manager, as neither objectivity nor impartiality can be maintained. Secondly, sufficient time must be made available to the ISO for his/her task. The time off must take into account that more time must be granted during the introduction of the project than the time granted during regular operations. This should be fixed separately in the role description. Thirdly, the formation of an information security team is an essential part of establishing, implementing, and maintaining an information security process.

The following individuals or officers must be appointed to the core information security team, and all of them should report to the top management for the decisions and necessary resources:

Risk manager

This role should consider all risks the SME can face (physical, legal, contractual, informational, IT, etc.). The risk manager is responsible for:

- gathering information about threats and vulnerabilities related to these;
- computing the risk level based on the likelihood of an event occurring and the severity of the operational impact and consequence to the business in case of occurrence;
- analysing potential remedies and controls to cope with these risks;
- keep top management informed on the situation and receive from them the necessary decision and resources.

Information security manager

This role concerns all types and media supporting information, and their management. The information security manager is responsible for:

- coordinating with the risk manager in relation to the risks to information – they can, if sufficiently trained, perform information security risk management on behalf of the risk manager;
- preparing, coordinating, and monitoring the information security actions plan that has been decided by the top management;
- preparing, coordinating, and monitoring the Awareness and Training program.

Incident manager

This role concerns all types of incidents and especially these related to information in the application of control #4. The incident manager works in close relation with the information security manager and is responsible for:

- establishing the list of events that the SME wants to control;
- preparing and proposing:
  - criteria to promote an information security event to an incident;
  - a set of actions and resources to control the incident;
  - procedures and mechanisms to raise the event to point of contact;

- proposing:
    - the structure and required skills of the incident response team (IRT). It is to be noted that several IRTs can exist depending on the type of incident, source, and consequence;
    - the creation of a role of 'incident handler' who coordinate the activities of the IRTs;
    - a process to learn from incidents aiming to reduce future occurrence and/or to improve the response.
- criteria to declare the incident as closed;
- keeping all events and incidents in a registry/database.

Vulnerability manager

This role concerns ICT vulnerabilities and especially those that apply to critical ICT components. The vulnerability manager works in close relation with the risk manager and the information manager and the incident manager. He/she is responsible for:

- identifying vulnerabilities and communicating these to the risk manager;
- preparing and proposing solutions to remove the vulnerabilities;
- helping the incident manager to build the response to the incident caused by or introduced by the vulnerabilities.

Problem manager

This role concerns all events, situations and conditions that do not immediately hit the information security objectives but can jeopardise them if combined. It tackles the non-ICT part of the vulnerabilities SMEs could face and their responsibility is very close to the vulnerability manager. The problem manager has to:

- identify these events and conditions;
- elaborate workarounds to allow preservation of the business operations while 'repairing' the situation.

Crisis manager

This role concerns situations that seriously hit business capability when a key role is unexpectedly absent to make a decision or act as predefined, or when a key process (or key technological component allowing its operation) is defective. The close coordination with the incident manager and the risk manager is mandatory as, here, the potential consequence is the end of the business. This role is responsible for:

- identifying situations and conditions that may negatively affect business objectives;
- evaluating the duration of the interruption of service/operation — or loss of data —, that is considered as 'borderline' to achieving the business objectives;
- analysing and proposing workarounds, procedures and needed resources to allow building business and technological resilience.

Compliance manager

This role concerns all business and operational aspects that are ruled by laws or contractual requirements. This role should be allocated to a member of the direction committee. The compliance manager is responsible for:

- identifying laws and contractual requirements;
- identifying defaults in conformity and propose remedies;

- communicating regularly with the other roles to promote compliance.

Privacy

***Data protection officer (DPO)*:**

The DPO is a compliance manager in the application of the GDPR. This role is mandatory as soon as PIIs are processed by the SME. The DPO should be independent of any decision role or committee within the SME.

CONTROL #16 ADDITIONAL PRIVACY CONTROLS

Control

Here are some specific privacy controls that can be relevant for the requirements of processing personal data for an SME.

This control is based on ISO/IEC 27701 “Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines” and complements the general security controls described in the previous controls and relevant specialisations on privacy, when present. The goal is to provide a tool that allows the SME to perform an initial assessment to identify potential compliance issues with GDPR. Addressing those issues requires specialised support.

Aim

In general, the requirements of ISO/IEC 27001:2013 mentioning "information security" shall be extended to the protection of privacy as potentially affected by the processing of personal data. The case of an SME acting as the processor processing personal data on behalf of the controller is not considered. This

is because the principles are the same but is typically a context where the processing of personal data is the core business of an SME and is too complex to be covered significantly by a simplified guide and is likely to require an in-depth analysis.

Scope

This set of controls concern the processing of personal data for an SME acting as the controller. This covers cases where it is required to determine the purposes and means of the processing of personal data.

Situation

The objective of the privacy controls described in this section is to allow to address the following issues:

- **conditions for collection and processing of personal data**: SMEs should determine and document that processing of personal data is lawful and has legal basis according to GDPR or specific legislation, with purposes that are clearly defined and legitimate;
- **obligations to data subjects:** SMEs should ensure that appropriate information is provided to data subjects about the processing of their personal data and that any other obligations applicable to data subjects in relation to personal data processing are met;
- **privacy by design and privacy by default**: SMEs should ensure that processes and systems are designed such that collection and processing of personal data (including use, disclosure, retention, transmission, and disposal) are limited to what is necessary for the identified purpose;
- **personal data sharing, transfer, and disclosure**: SMEs should determine and document when personal data is transferred to other jurisdictions or third parties and/or disclosed in accordance with applicable obligations.

Guidance

A. **Conditions for collection and processing of personal data**

This set of controls covers the conditions for the collection and processing of personal data:

- identify and document the specific purposes for which personal data is processed;
- determine, document, and comply with GDPR and any applicable legislation (for example

the ePrivacy directive or forthcoming regulation) for the identified purposes;

- obtain and record consent from data subjects according to documented processes by which it can be demonstrated if, when and how consent was obtained;
- assess the need for, and implement where appropriate, a privacy impact assessment whenever new processing or change to existing processing of personal data is planned;
- ensure that written contracts are in place with any personal data processor that is used, ensuring that they address the implementation of the appropriate controls;
- determine respective roles and responsibilities for the processing of personal data in case of any joint personal data controller;
- determine and securely maintain the necessary records in support of its obligations for the processing of personal data.

B. **Obligations to data subjects**

This set of controls covers the obligations to data subjects:

- determine and document legal, regulatory, and business obligations to data subjects related to the processing of their personal data and provide the means to meet these obligations;
- determine and document the information to be provided to data subjects regarding the processing of their personal data and the timing of such a provision;
- provide data subjects with clear and easily accessible information identifying the controller and describing the processing of their personal data;
- provide a mechanism for data subjects to modify or withdraw their consent and to object to the processing of their personal data;
- implement policies, procedures and/or mechanisms to meet their obligations to data subjects to access, correct and/or erase their data;
- inform third parties with whom personal data has been shared of any modification, withdrawal or objections pertaining to the shared personal data, and implement appropriate policies, procedures and/or mechanisms to do so;
- be able to provide a copy of the personal data that is processed upon request by the data subject;
- define and document policies and procedures for handling and responding to legitimate requests from data subjects;
- identify and address (legal) obligations to the data subjects resulting from decisions related to the data subject based on automated processing of personal data.

C. **Privacy by design and privacy by default**

This set of controls covers the “privacy by design” and “privacy by default”:

- limit the collection of personal data to the minimum that is relevant, proportional, and necessary for the identified purposes;
- limit the processing of personal data to that which is adequate, relevant, and necessary for the identified purposes;
- ensure and document that personal data is as accurate, complete, and up to date as is necessary for the purposes for which it is processed, throughout the life cycle of the personal data;
- define and document data minimisation objectives and what mechanisms (such as pseudonymisation[18]) are used to meet those objectives;

18 As defined by GDPR: replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified.

- either delete personal data or render it in a form which does not permit identification or re-identification of data subjects, as soon as the original personal data is no longer necessary for the identified purpose(s);
- have documented policies, procedures and/or mechanisms for the disposal (e.g., erasure or destruction) of personal data and ensure that temporary files created as a result of their processing are disposed following documented procedures within a specified, documented period;
- do not retain personal data for a longer time period than the time necessary for the purposes of the personal data is processing;
- subjecting transmitted personal data over a data-transmission network to appropriate controls designed to ensure that the data reaches its intended destination.

D. **Personal data sharing, transfer, and disclosure**

This set of controls covers the personal data sharing, transfer, and disclosure:

- identify and document the relevant basis for transfers of personal data between jurisdictions;
- specify and document the countries and international organisations to which personal data can possibly be transferred;
- record transfers of personal data to or from third parties and ensure cooperation with those parties to support future requests related to obligations to the data subjects;
- record disclosures of personal data to third parties, including what personal data has been disclosed, to whom and at what time.

8. CONCLUSION

Using enabling technologies to innovate, produce, and provide solutions is becoming increasingly part of every SME's business processes and naturally corresponds to the long term goal of digital transformation including a basic level of digital intensity for most European SMEs as communicated by the DIGITAL DECADE. However, cybersecurity remains a major concern for SMEs and one of the main threats of business continuity and survival!

As security threats are recurring, an information security process is needed to protect three fundamental values: confidentiality, integrity, and availability of information. Therefore, Information Technology and Cybersecurity have become a fundamental prerequisite for the personal development of individuals and economy in the European Union and worldwide. Certain prerequisites are necessary to establish information security in an enterprise in order to ensure and maintain the required level of compliance.

Protecting information is a crucial part of cybersecurity policies, guidelines, recommendations, and standards to ensure compliance. The ISO/IEC 27002 is one of many resources dealing with data protection. However, it is a complex document that many SMEs would find it hard and costly to implement. This guide helps SMEs in implementing the minimum recommended controls to protect their information, maintain consumers' trust, and comply with GDPR rules. Section 7 remains largely a technical section that ICT and cybersecurity SME professionals – the digital enablers - would use to help SMEs implement the recommended controls to reduce the risk of cybersecurity attacks.

This guide's primary target is SMEs (non-ICT) who need to understand the importance of protecting information and complying with different laws, including GDPR. Hence, this guide aims to raise awareness among SMEs and guide SMEs management through an effective strategy and policy for data protection. ICT SMEs and professionals can refer to section 7 for more technical information on the implementation

of the 16 security controls and use this information to assist and advice SMEs on the most appropriate action(s).

This guide showed how Standards would help SMEs secure their information in a quick and cost-effective manner. It also pointed out to the need for SMEs to be aware of GDPR compliance since they process personal information in many situations. In that respect, it focused on privacy protection as an important pillar of GDPR, where processing and free movement of personal data is balanced with the protection of the fundamental rights and freedoms of people, notably their right to protect their personal data; i.e., protecting their privacy.

The guide also argued that effective implementation of security control is not possible without a sound security strategy and clear security objectives. While standards (and controls) - ISO/IEC 27014 in this case - focus on what an enterprise needs to implement, there is little reference on how to implement it. Therefore, specialised knowledge is needed to bring the strategy defined by the governing body to the concrete and measurable processes and procedures through COBIT.

Finally, it introduced 16 security controls as the minimum recommended controls, in which SMEs need to implement in order to protect their information and comply with GDPR rules. These controls address personal, organisational, and technical issues to ensure comprehensive protection related, among other things, to:

1. Manage and protecting digital assets
2. Respond to cyber attacks
3. Establish policies for data sharing, backup, and remote working
4. Ensure safeguards to minimise vulnerabilities and cyberthreats and maintain business continuity after a cyberattack

ANNEX A: INFORMATION CLASSIFICATION TECHNIQUE

1. Introduction

As mentioned in the introduction of this guide, we know that information has various goals or objectives. The business processes are there to achieve these goals and sometimes, it is input information that is the most important, sometimes it is the output, sometimes both inputs and outputs.

The value of information should be defined in terms of business objectives or the consequences if these objectives are not achieved.

Four axes to measure the value have been identified:

- **Own value**: what it costs to acquire and maintain the information; for example, what is directly available on the internet is free and requires no maintenance; a database with its metadata that must remain up to date is another story;
- **Usage value**: the amount and importance of what we can do if the information fits our needs; this is in direct relation with the business objectives; for example, a car allows us to travel to meet clients, or go on holiday;
- **Loss value**: what we cannot do anymore if the information quality is degraded or if the security criteria are no more achieved; for example, a blown tire or a lack of fuel blocks us in our move and we can miss an opportunity or a contract, or we miss our plane with financial consequences… the car is however always there and can be repaired;
- **Attraction value**: how interesting the information we need could be to 'others' to prevent us to reach our objectives… or reaching them before us.

These four axes do not have the same weight with regards to the security criteria (confidentiality, integrity, availability).

The value of information should be evaluated for each security criteria.

2. Procedure

2.1 To be done in team with the top management

1. List the Stakes in decreasing order of importance for the enterprise (see Table 1).
2. Establish qualitative consequence gravity scales in case the stakes and values were damaged (four levels should suffice – a pair number prevents the simplistic use of an average position chosen when we do not know, see Table 2).
3. Create categories of information of the same kind (financial, operational, related to persons…) or related to the same business process/activity, and choose one representative information for each category.
4. List the TEN most important business processes for the enterprise (ordered in decreasing order) to achieve its objectives, with the three to five key information (as input or output).
5. Identify three to five key ICT components that allow reaching the objectives of the listed processes.

Reproduce this procedure at least once a year, maybe with different processes and information to make sure all the key information categories have not been classified. By this procedure, we identify and classify

(evaluate the value) the categories of information requiring protection. Once the key information is classified, all information of the category will receive the same value and, hence, the same level of protection.

Some key categories could be associated with key business processes; they should however be adequately protected. Here, what matters is the category of information, not the key process.

Note: The business process receives the classification level of the most valued information. The ICT components inherit the classification level of the process they support or the information they contain. This is essential to determining their business criticality for the Business Continuity Plan (BCP) and the incident management.

2.2 To be done by the 'owner' of the business process

For each chosen process or information

- Determine the stakes that will be damaged if the result of the business process/activity does not reach the expectations (for the enterprise or the client). Each process of information will probably come out with a different set of stakes.
- Determine, for each chosen information, using Table 2, the need for protection/security in terms of confidentiality, integrity, and availability. The need for security will be inherited by all information within the category represented, be them already used or new (acquired or produced).
- Protect the information according to the need for security.

This procedure should be repeated at least once a year because many things can change in the context of the enterprise or its objectives.

A. Stakes

Stakes are, like in poker or in a bet, what we lay on the table and that we do not want to lose.

There are **nine** types of stakes, each potentially containing different levels:

Stake	Level
Reputation	• Loss of internal thrust • Loss of external image or credibility • Loss of technological reputation (competences, skills) • Loss of competitive advantage • Loss of technological leadership • Loss of negotiation capability
Legal or judicial consequences	• Legal non-conformity • Inability to satisfy to legal obligations • Negative effect on the general abiding to the law • Judicial conflict • Judicial suits and/or fines

Stake	Level
Breach of privacy	• Reduction of people' capacity to continue a normal personal, familial, social, judicial and economical life • Difficulty to find a job
Financial loss (direct or indirect)	• Financial losses (as a consequence of the event) • Emergency and repair (HR, equipment, studies, appraisal, etc.) costs • Loss of market shares • Loss of good or assets • Loss of clients/customers
Social or industrial problems	• Social crisis – Strike • Forced resignation • Dismissal • Enterprise closure • Long duration unemployment
Operational impact	• Interruption of service (as a result of the event, e.g., as long as the problem is not resolved) • Loss of internal effectiveness, internal operational disturbances/disruptions • Internal organisational difficulties (reorganisation, loss of human resources, etc.) • Loss of providers
Contractual problems (with clients or providers)	• Third parties' operational disturbances/disruptions • Contractual difficulties • Inability to respect contractual clauses
Physical Endangering of people (health, injuries, death)	• Weakening of the capacity to adequately protect people • Endangering environment (pollution) weakening of the capacity to preserve the environment and to fight pollution
Breach to the confidentiality of entrusted information (classified or owned by third parties)	

Table 1: Stakes

You will need to select several impacts to evaluate the value of information:

- at least THREE (3) to acquire a non-linear view of the situation and allow a general sight less sensible to the obvious (that are frequently misleading) and more stable along the flowing time;
- maximum FIVE (5) to keep the evaluation manageable in the time.

B. Need for security

In Table 2, each security criterion is split in several questions.

• Confidentiality: when the process requires it, it is important to split into the input and output information. Depending on the category of information and the size of the enterprises, it would be essential to separate the confidentiality breaches to internal people (not involved with the process) and the external world.

• Integrity: we should look for the need related to the input information and the output, which also considers the integrity problem of the (automated) process.

• Availability: it is essential to segregate the consequence (and the need for protection) due to short time problems (disturbances) from these related to long term events (including destruction). Table 3 allows making a clear delineation between both durations.

0	No effect
1	Sensible effect but without consequence; low impact
2	Acceptable and manageable effect; moderate impact
3	Hardly acceptable and manageable effect; high impact
4	Catastrophic effect impossible to manage; exceptional impact

Table 2: Impact level on the stakes

Criterion/Damage	**Stake 1**	**Stake 2**	**Stake 3**	**Stake 4**	**Stake 5**	**Security need**
Confidentiality	**0**	**0**	**0**	**0**	**0**	**0**
Internal compromission of input information						0
Internal compromission of output information						0
External compromission of input information						0
External compromission of output information						0
Integrity	**0**	**0**	**0**	**0**	**0**	**0**
Erroneous output date						0
Erroneous input date						0
Availability	**0**	**0**	**0**	**0**	**0**	**0**
Acceptable unavailability						0
Unacceptable unavailability						0
TOTAL (criterion)	**0**	**0**	**0**	**0**	**0**	**0**

Table 3: Classification of information

Note: on each line in Table 2, as for each criterion (two lines), the 'need for security' is the maximal value obtained. It is, indeed, the strongest need that has to be taken into account.

You will easily discover that the stakes and obtained values can be different for each (category of) information and related process. This is an objective to reach and will remain independent from the selected security controls implemented to cover the risks.

Unavailability duration (for information or technology)	**Level of harm**	**AAF**	**AUD**	**MAU**
≤ 5 minutes				
≤ 30 minutes				
≤ 1 hour				
≤ ½ day				
≤ 1 day				
≤ ½ week				
≤ 1 week				
≤ ½ month				
≤ 1 month				

Table 4: Determination of the threshold between short and long unavailability

AAF: Annual Acceptable Frequency

AUD: Annual Unavailability Duration: Unavailability duration x AAF.

MAU: Mean value of the Annual unavailability (AUD) – the sum of the different AUDs / 9. Everything below this threshold is acceptable in table 2, what is above, is unacceptable.

C. Protection of information

The protection level can be defined in general terms:

0	No
1	Elementary
2	Good practices
3	Best practices
4	State of the art

Levels 4 and 3 should be first ensured. The other needs will be naturally covered by the taken controls, at least in the first months. Other controls can be added if surveillance shows the need.

Note: in addition to their business importance to achieve the objectives, processes inherit from the value (and protection) of the information they process or create.

ICT assets inherit from the classification level of the processes and information they contain.

For each criterion, the protection level also possesses a more precise and practical meaning. Each protection level builds on the previous one.

Confidentiality

1	Accessible to all enterprise/organisation's personnel or on a need-to-know basis. Should not exit the enterprise/organisation's premises and systems without a need to know (need to share). Appropriate Non-Disclosure agreements must be in place.
2	Only authorised personnel may have access on a need to have basis. Distribution list must be mastered. This applies for instance to information needed for the daily operations, but protected by law, such as call data records.
3	Discretionary access control (DAC). Information cannot leave the enterprise/organisation's premisses without approval of asset owner and appropriate control (encryption or physical access control). Storage in controlled environments. Encryption recommended. Stored at rest in locked cabinets at least when printed, in database and file systems. Isolation of 'elements' is not mandatory (Confidential information may be stored in the same instance of a database as non-confidential information as long as the appropriate level of access control is in place). Data may be stored in the Cloud as long as: 1) the cloud service provider has successfully been vetted from a security / risk management point of view; 2) at least the same level of User identification, identity and access management are in place (compared to in-house at the enterprise/organisation).
4	Access to the data is strictly controlled, i.e., Mandatory access control (MAC). Each element is isolated from the others in a very strong individual container: different instances of databases (with encryption) for different types of datasets. The data must be stored in a safe or vault. Encryption required. Information and may not be taken out of the premisses without a very strong physical container. Transmission of the physical data to individuals must be logged. Physical information should be individualised whenever possible (unique numbers, copies to registered individuals, etc.) Per default, highly confidential data is not to be stored or processed in the cloud, unless appropriate authentication and encryption mechanisms are in place. These mechanisms (and the architecture of the proposed implementation) will always have to be reviewed and approved by Security Management.

Integrity

1	None
2	Managed: Integrity is verified by the user at the source or at the end of the process; information is corrected when discrepancy is found, under directives and within time frames defined by the owner. Backups are a way to recover correct information.
3	Controlled: Prevention of integrity problems on the whole process; Detection a posteriori (in a short delay to be defined by the owner); issues are to be signalled to the asset owner. This control is provided for instance per default by the database systems and by the secure storage systems. Read-only documents, except for authorised personnel.
4	Unalterable: Integrity problems are avoided. Mandatory integrity controls on the documents and databases (hash/Checksum); documents are stored in unalterable format. Detection in Real Time. Issues are immediately signalled to the owner who controls the correction.

Availability

1	None RTO: 7 days; RPO: 3-7 days
2	A replacement is foreseen; replacement is planned and happens according to conditions defined by owner or responsible authority. RTO: < =48 hr; RPO: <= 24 Hr
3	Proactive maintenance is recommended. Status is monitored. Unavailability is planned and replacement realised in a short delay defined by the responsible authority. RTO: < 24 Hr; RPO: < 8 Hr
4	Unavailability is avoided and the replacement is immediate; Systems are fully redundant, and data is replicated in (quasi) real time (mirroring or log shipping techniques). Proactive maintenance is mandatory on systems and applications. The system is continuously managed and monitored. Very high important system and application support contracts are in place (Gold, platinum or custom made). RTO: < 4 Hr; 0<= RPO <= 15 minutes, depending on the technology available.

°RTO (Recovery Time Objective): is the maximum amount of time allowed to resume an activity, recover resources, or provide products or services after a disruptive incident occurs. This target time period must be short enough to ensure that adverse impacts do not become unacceptable.

°RPO (Recovery Point Objective): Point in time in the past to which the information or its processing shall be restored after a disruptive incident occurs in order to allow an activity to resume after a disruptive incident has occurred. In other words: how much information may be lost (from the last changes or updates) without causing too much trouble.

RPO is taken to guarantee RTO is achievable, but also to document the quantity of information or processing that can be lost in case of disruption.

Access control to information also follows the evaluated need for protection.

Access Control

1	Accessible to the enterprise/organisation personnel; standard access control is applicable One factor-based authentication.
2	Role based controlled access (RBAC); only authorised personnel get access, and these are logged = only for Restricted information.
3	Discretionary access control (DAC); authorised personnel can access when needed, transmission (if justified) is allowed under permission of owner. Two-factor authentication.
4	Mandatory access control (MAC); individual access; transmission request must be justified and is made by the owner. Multi-factor authentication (2 or more).

RBAC (Role based access control) is a mode by which the users are given a functional profile whose rules are set in the systems

DAC (Discretionary access control) is a mode by which the asset owner determines the access rules for identified individuals and whose control is delegated to the asset manager.

MAC (Mandatory access control) is a mode by which the asset owner not only defines but manages the access rules (no delegation).

There are three kinds of authentication factors: something you know (e.g., a password), something you have (e.g., a token or key) and something you are (e.g., biometrics). Three-factor authentication (combining the three modes) is used only exceptionally and is not commonly seen in commercial organisations.

ANNEX B: LISTING OF THE CONTROL TITLES WITH THEIR NUMBER, PER REFERENCE

The main reference is ISO/IEC JTC1 SC27 27002:2013 “Code of practice for information security controls.”

The newest version of the standard: ISO/IEC 27002:2022" contains different section numbers. If you use the newest version, you can consult the corresponding section numbers on this page.

Section in this guide	ISO Reference
5. Privacy protection	ISO/IEC 27701
6. Information security governance	ISO/IEC 27014
Control #1 Asset management	ISO/IEC 27002 8.1.1 Inventory of assets 8.1.2 Ownership of assets 8.2.1 Classification of information 8.2.2 Labelling of information 8.2.3 Handling of assets 8.3.2 Management of removable assets Disposal of media 8.3.3 Physical media transfer
Control #2 Policies, standards and guidelines	ISO/IEC 27002 5.1.1 Policies for information security 5.1.2 Review of the policies for information security
Control #3 Incident management	ISO/IEC 27002 16.1.1 Responsibilities and procedures 16.1.2 Reporting information security events 16.1.4 Assessment and decision on information security events 16.1.5 Response to information security incidents 16.1.6 Learning from information security incidents ISO/IEC 27035-1 “Information security incident management – Part 1 Principles and process”
Control #4 Access control management	ISO/IEC 27002 9.1.1 Access control policy 9.2.1 User registration and de-registration 9.2.2 User access provisioning 9.2.3 Management of privileged access 9.2.4 Management of secret authentication information of users 9.2.5 Review of access rights
Control #5 Network security and data exchanges	ISO/IEC 27002 13.1.1 Network controls 13.1.3 Segregation in networks 13.2.1 Information transfer policies and procedures 13.2.2 Agreements on information transfer 13.1.4 Confidentiality or non-disclosure agreements ISO/IEC 27010 “Information security management for inter-sector and inter-organizational communications”

Section in this guide	ISO Reference
Control #6 Vulnerability management	ISO/IEC 27002 12.6.1 Management of technical vulnerabilities 12.6.2 Restriction on software installation 16.1.3 Reporting information security weaknesses
Control #7 Fighting malware	ISO/IEC 27002 12.2.1 Controls against malware
Control #8 Backup management	ISO/IEC 27002 12.3.1 Information backup
Control #9 Safeguards management	
Control #10 ICT readiness for business continuity	ISO/IEC 27002 17.1.1 Planning information security continuity 17.1.2 Implementing information security continuity 17.1.3 Verify, review, and evaluate information security continuity ISO/IEC 27031 “ICT readiness for business continuity”
Control #11 Remote working	ISO/IEC 27002 6.2.1 Mobile device policy 6.2.2 Teleworking
Control #12 Cyber threats watch	
Control #13 Information security awareness	ISO/IEC 27002 7.2.2 Information security awareness, education, and training
Control #14 Information security aspects in relations to suppliers	ISO/IEC 27002 15.1.1 Information security policy for supplier relationships 15.1.2 Addressing security within supplier agreements 15.1.3 Information and communication technology supply chain 15.2.1 Monitoring and review of supplier services 15.2.2 Managing changes to supplier services **ISO/IEC 27036-1 “Information security for supplier relationships — Part 1: Overview and concepts”**
Control #15 Information security organisation	ISO/IEC 27002 6.1.1 Information security roles and security 6.1.2 Segregation of duties
Control #16 Additional privacy controls	ISO/IEC 27701

ANNEX C: COBIT PROCESSES AND SECURITY MANAGEMENT

Each of the five COBIT domains contain multiple processes. All these processes contain the following structure:

- Process:
  - Description and purpose.
  - Enterprise goals and metrics.
  - IT goals and metrics.
- Management practices:
  - Management practice description.
  - Metrics.
  - Tasks based on capability level.
- Organisational structures (RACI matrix).
- Information flows and items.
- People, skills, and competencies.
- Policies and procedures.
- Culture, ethics, and behaviour.
- Services, infrastructure, and applications.

Following the steps of this methodology, we will be able to implement security controls, aligned with the strategy and business objectives, and we will obtain very valuable information on the efficiency of security controls.

The following table shows the different COBIT domains and processes, and their correspondence with the set of security controls most used in Europe, which is the ISO/IEC 27001: 2013 standard.

COBIT PROCESS		**ISO/IEC 27001**
EDM	**Evaluate, Direct and Monitor**	
	01 Ensured governance framework setting and maintenance	4.3 Determining the scope of the information security management system 5 Leadership 6.2 Information security objectives and planning to achieve them A.5 Information security policies
	02 Ensured Benefits Delivery	9.3 Management review 10 Improvement
	03 Ensured Risk Optimisation	6.1 Actions to address risk and opportunities 8.2 Information security risk assessment 8.3 Information security risk treatment
	04 Ensured Resource Optimisation	7.1 Resources 7.2 Competence 7.3 Awareness 7.5 Documented information A.6.1 Internal organisation

	05 Ensured Stakeholder Engagement	4.1 Understanding the organisation and its context 4.2 Understanding the needs and expectations of interested parties 7.4 Communication
APO	**Align, Plan and Organise**	
	01 Managed the IT Management Framework	4.4 Information security management system 5 Leadership A.5 Information security policies 8.1 Operational planning and control
	02 Managed Strategy	4.4 Information security management system 6.2 Information security objectives and planning to achieve them
	03 Managed Enterprise Architecture	A.9 Access control A.11 Physical and environmental security A.12 Operations security A.13 Communications security
	04 Managed Innovation	
	05 Managed Portfolio	
	06 Managed Budget and Costs	8.3 Information security risk treatment
	07 Managed Human Resources	7.1 Resources 7.2 Competence 7.3 Awareness A.7 Human resource security
	08 Managed Relationships	4.2 Understanding the needs and expectations of interested parties 7.4 Communication A.6.1 Internal organisation
	09 Managed Service Agreements	4.2 Understanding the needs and expectations of interested parties 7.4 Communication A.15 Supplier relationships
	10 Managed Vendors	A.13.2 Information transfer A.14 System acquisition, development, and maintenance A.15 Supplier relationships A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.4 Privacy and protection of personally identifiable information
	11 Managed Quality	9 Performance evaluation 10 Improvement
	12 Managed Risk	6.1 Actions to address risk and opportunities 8.2 Information security risk assessment 8.3 Information security risk treatment
	13 Managed Security	Dealt with throughout ISO/IEC 27001

	14 Managed Data	A.8 Asset management A.10 Cryptography A.12 Operations security A.18.1.4 Privacy and protection of personally identifiable information
BAI	**Build, Acquire and Implement**	
	01 Managed Programs	
	02 Managed Requirements Definition	4.2 Understanding the needs and expectations of interested parties
	03 Managed Solutions Identification and Build	A.14 System acquisition, development, and maintenance
	04 Managed Availability and Capacity	A.12.1.3 Capacity management
	05 Managed Organisational Change	A.12.1.2 Change management
	06 Managed IT Changes	A.12.1.2 Change management
	07 Managed IT Change Acceptance and Transitioning	A.12.1.2 Change management A.14 System acquisition, development, and maintenance
	08 Managed Knowledge	7.5 Documented information A.12.1.1 Documented operating procedures A.16.1.6 Learning from information security incidents
	09 Managed Assets	A.8 Asset management
	10 Managed Configuration	A.9 Access control A.12 Operations security
	11 Managed Quality	9 Performance evaluation 10 Improvement
DSS	**Deliver, Service and Support**	
	01 Managed Operations	8.1 Operational planning and control
	02 Managed Service Requests and Incidents	A.16 Information security incident management
	03 Managed Problems	A.16 Information security incident management
	04 Managed Continuity	A.17 Information security aspects of business continuity management
	05 Managed Security Services	Dealt with throughout ISO/IEC 27001
	06 Managed Business Process Controls	9 Performance evaluation
MEA	**Monitor, Evaluate and Assess**	
	01 Managed Performance and Conformance Monitoring	9.1 Monitoring, measurement, analysis, and evaluation 9.3 Management review
	02 Managed System of Internal Control	9.2 Internal audit 4.2 Understanding the needs and expectations of interested parties A.18 Compliance

	03 Managed Compliance with External Requirements	9.2 Internal audit 4.2 Understanding the needs and expectations of interested parties A.18 Compliance
	04 Managed Assurance	9.3 Management review

ANNEX D: A LIST OF COMPUTER EMERGENCY RESPONSE TEAM (CERTs)

Country	Name
Austria	CERT.at (Austrian National CERT)
Belgium	Centre for Cyber Security Belgium
Bulgaria	Bulgarian National Center for Incident Response in Information Security
Cyprus	National CSIRT-CY
Denmark	Centre for Cyber Security (CFCS)
Estonia	CERT-EE (Estonian National CERT)
Finland	Finnish National Cyber Security Centre
France	French National Cyber Security Agency, In English
Germany	CERT-Bund (German National CERT), link 2
Greece	Hellenic CSIRT
Hungary	National Cyber Security Centre of Hungary
Ireland	IRISS
Italy	Italian National Cybersecurity Agency
Latvia	Information Technology Security Incident Response Institution
Malta	Government CSIRT of Malta
Poland	CERT POLSKA (Polish CERT)
Portugal	Portuguese National Cyber Security Centre
Romania	Romanian National Directorate for Cybersecurity
Slovenia	SI-CERT (Slovenian National CERT)
Spain	Spanish National Cybersecurity Institute
Switzerland	Swiss National Cybersecurity Centre
Netherlands	Dutch Digital Trust Center
United Kingdom	UK's National Cyber Security Centre

BIBLIOGRAPHY

ENISA (2015). *National/governmental CERTs - ENISA's recommendations on baseline capabilities*. ENISA. Retrieved from https://www.enisa.europa.eu/publications/national-governmental-certs-enisas-recommendations-on-baseline-capabilities

European Commission. (2020). E*urope's Digital Decade: digital targets for 2030. Brussels: European Commission*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (Retrieved December 21, 2021).

Eurostat. (2019). *ICT security in EU enterprises*. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ICT_security_in_enterprises#ICT_security_in_EU_enterprises (Retrieved December 21, 2021).

ISACA. (2019). *COBIT for Small and Medium Enterprises Using COBIT 2019*. ISACA.

International Organization for Standardization. (2021, December 21). I*SO 9000 FAMILY*

QUALITY MANAGEMENT. International Organization for Standardization. https://www.iso.org/iso-9001-quality-management.html

International Organization for Standardization. (2020). *Information security, cybersecurity and privacy protection — Governance of information security*. (ISO/IEC 27014:2020). https://www.iso.org/standard/74046.html

International Organization for Standardization. (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* (ISO/IEC 27701:2019). https://www.iso.org/standard/71670.html

International Organization for Standardization. (2018). *Information technology — Security techniques — Information security risk management*. (ISO/IEC 27005:2018). https://www.iso.org/standard/75281.html

International Organization for Standardization. (2015). *Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements*. (ISO/IEC 17021-1:2015). https://www.iso.org/standard/61651.html

International Organization for Standardization. (2013). *Information technology — Security techniques — Information security management systems — Requirements*. (ISO/IEC 27001:2013). https://www.iso.org/

standard/54534.html

International Organization for Standardization. (2022). *Information security, cybersecurity and privacy protection — Information security controls.* (ISO/IEC 27002:2022). https://www.iso.org/standard/75652.html

International Organization for Standardization. (2013). *Information technology — Security techniques — Code of practice for information security controls*. (ISO/IEC 27002:2013). https://www.iso.org/standard/54533.html

International Organization for Standardization. (2012). *Conformity assessment — Requirements for bodies certifying products, processes and services*. (ISO/IEC 17065:2012). https://www.iso.org/standard/46568.html

Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. In *ARES 2021: The 16th International Conference on Availability, Reliability and Security* (pp. 1-7). Vienna; Association for Computing Machinery. Retrieved 21 December 2021, from https://dl.acm.org/doi/pdf/10.1145/3465481.3469200.

Regulation (EU) 2016/679. *The protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. European Parliament, Council of the European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Small Business Standards (SBS). (2017). *SME Guide for the Implementation of ISO/IEC 27001 on Information Security Management*. Brussels: SBS. Retrieved from https://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

ABOUT THE EXPERTS

Chairman: Jean-Luc Allard

Industrial Engineer, MSC (retired). Former officer of the Belgian Air Force. Expert in information security governance and management with 25 years of experience. Active in standardisation (ISO/IEC JTCI SC27) since 2002.

Free-lance consultant in formation security governance and management.

Coordinator: Omar Dhaher

Senior Technology Manager at DIGITAL SME. Coordinator of DIGITAL SME WG Standards and WG SBS Digitalisation. Member of the Task Force Rolling Plan of EC's Multi Stakeholders Platform on ICT Standardisation. Experienced in ICT, industrial policy with reference to Telecommunications Regulatory Frameworks, entrepreneurship, work-based learning, digital skills, research, and standardisation.

Members

Andrea Caccia: Senior Consultant, Project Manager, Standard and regulation compliance, product development coordinator on:

- Trust Services, and all related product and technologies, e.g., eSignature, eSeal, eDelivery
- electronic Invoicing and archiving
- blockchain & DLT

Andrea participates in the most important European Standardization activities (ETSI, CEN, ISO, UNI/UNINFO, OASIS)

Daniele Tumietto

Independent consultant, senior advisor, innovation manager. Daniele is also an adjunct professor at the Link Campus University in Rome (Italy) and O.M. Beketov University in Kharkiv (Ukraine).

Member of several National, European, and International Standard technical committees in e-invoicing, e-procurement, eBusiness and financial services, eIDAS, privacy and personal data protection, Blockchain & DLT, Industry 4.0, Quantum technologies, AI, Circular Economy and ESG.

Davide Giribaldi

CEO of EnCybeRisk srl - Senior GRC & Information Security Advisor – Coordinator of Assintel Cybersecurity Working Group with a deep knowledge within the field of Enterprise Security Risk Management. Davide has 27 years' experience in critical contexts, to ensure business continuity and crisis management for Italian Public Bodies and large multinational corporations.

Francisco Menéndez

Francisco is an Information Security, Services Management and Business Continuity specialist and the head of Information Security and Compliance Services at Seresco. He is a lead auditor of ISO 27001, ISO 28000, ISO 20000-1, and ISO 22301. ISACA Platinum member. ISACA certifications: CISA, CISM, CRISC and COBIT Foundation. Francisco is the coordinator and member of the itSMF Spain workgroup and member of the Industrial Cybersecurity Centre workgroup.

Samuel Fricker

Professor at the University of Applied Sciences Northwestern Switzerland and the coordinator of the Horizon-2020 project GEIGER[19]. GEIGER aims at bringing cybersecurity to small and medium-sized enterprises in cooperation with the European DIGITAL SME Alliance, ENISA, ECSO and diverse national actors. Samuel holds a PhD from the University of Zurich.

19 Contributions made by the project GEIGER to this guide received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883588.

Small Business Standards

sbs-sme.eu

@sbs-sme

European DIGITAL SME Alliance

digitalsme.eu

@EUdigitalsme

European Commission

EFTA

Co-financed by the European Commission and EFTA Member States