ETSI TR 103 787-1 V1.1.1 (2021-05)

CYBER;
Cybersecurity for SMEs;
Part 1: Cybersecurity Standardization Essentials

Reference
DTR/CYBER-0061

Keywords
cybersecurity, framework, maturity assessment, SME

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
Executive summary 5
Introduction 6
1 Scope 8
2 References 8
2.1 Normative references 8
2.2 Informative references 8
3 Definition of terms, symbols and abbreviations 13
3.1 Terms 13
3.2 Symbols 13
3.3 Abbreviations 13
4 Background: What SMEs Need to Know About Cybersecurity? 14
5 The Five-Step Process to Establish and Improve Cybersecurity for SMEs 16
5.1 Introduction 16
5.2 (Step 1) Understand Your Company Profile 17
5.3 (Step 2) Perform Security Risk Assessment 18
5.4 (Step 3) Identify Applicable Security Controls (Risk Treatment) 18
5.5 (Step 4) Apply Security Controls (Risk Treatment) 19
5.6 (Step 5) Monitor and Improve 19
6 Five Cybersecurity Frameworks and Standards for SMEs and their Comparative Analysis 19
6.1 Introduction 19
6.2 Standards and Frameworks for Security Controls - A Comparative Analysis 21
7 Four Categories of SMEs in Cybersecurity Context 25
8 Exemplary Application: Cybersecurity Essentials for SME "UP" 26
Annex A: SME Standardization and the European Landscape 29
A.1 Introduction 29
A.2 EC Rolling Plan for ICT Standardization 29
A.3 Standards Developing Organizations (SDOs) 29
A.4 SME Organizations 29
A.5 Cybersecurity Organizations 30
Annex B: Starting with Standards and Standardization 31
B.1 What is a standard and what are the benefits of using standards? 31
B.2 How to search for the right standards? 31
B.3 How to get involved in the standardization processes? 31
Annex C: Standards Developing Organizations 32
C.1 International Standardization Bodies 32
C.2 European Standardization Organizations (ESOs) 32
C.3 National Standards Organizations (NSOs) 32

Annex D: Maturity Models for Cybersecurity and Information Security 34
D.1 What is a Maturity Model? 34
D.2 What are Examples of Maturity Models? 34
D.3 How Can Maturity Models Support Standardization? 34
Annex E: Bibliography 35
History 36

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

The present document is part 1 of a multi-part deliverable covering Cybersecurity for SMEs, as identified below:

Part 1: "Cybersecurity Standardization Essentials".

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The complexity of the cybersecurity domain and abundance of cybersecurity standards entail expertise, cost and complexity challenges for small and medium-sized enterprises (SMEs). The present document addresses and provides cybersecurity standardization guidance for different types of SMEs according to their roles in the digital ecosystem. Five widely used standards and frameworks that can be used to reduce the cybersecurity risks are introduced. A comparative analysis of these standards and frameworks is performed resulting in 17 unified cybersecurity control categories that serve as a quick reference for SMEs. The five-step process is illustrated by an exemplar SME to facilitate the implementation of the process. The present document can be used by SMEs as a "where-to-start" guideline for cybersecurity concepts, processes, standards and frameworks to initiate their own implementation.

Introduction

For the organizations that do not have prior cybersecurity experience, it is difficult to find a clue as to where to start their cybersecurity journey. Standards have been a trustworthy resource for individuals, organizations and governments who seek an answer to the question "What is the best way of doing this?" [i.1] and [i.2]. The International Standardization Organization (ISO) states several benefits of standards for small to medium sized enterprises (SMEs) [i.3]. According to ISO, standards can help SMEs to build customer confidence that their products are safe and reliable, to meet regulation requirements at a lower cost, to reduce costs across all aspects of their business, and to gain market access across the world.

As in every domain, standards on cybersecurity and information security are built on experience and best practices that can help organizations to cope with cyber threats. It might be difficult for SMEs to get into the almighty world of standards. To date, cybersecurity standardization of SMEs has received scant attention in the research literature [i.1]. Nevertheless, the European Standards Developing Organizations (CEN European Committee for Standardization (https://www.cen.eu/), CENELEC European Committee for Electrotechnical Standardization (https://www.cenelec.eu/) and ETSI European Telecommunications Standards Institute (https://www.etsi.org/)), SME Alliances (the European Digital SME Alliance (https://www.digitalsme.eu/), SBS Small Business Standards (https://www.sbs-sme.eu/)) and cybersecurity organizations (ECSO European Cyber Security Organization (https://ecs-org.eu/), ENISA) are putting in efforts to address the challenges that SMEs are facing.

In the present document, SMEs are provided with the essential information on where to start establishing cybersecurity by implementing standards and frameworks.

First, information on cybersecurity essentials by introducing the main concepts (i.e. threat, vulnerability, attack, control, risk, etc.) and their relationships is provided. This background information helps SMEs to follow the present document more easily.

Second, a five-step process that can be followed by SMEs to establish and improve cybersecurity using the standards and frameworks is proposed. This process provides SMEs with a quick-starting point. To facilitate the execution of the five-step process for different types of SMEs, the SME categories (see Table 1) proposed by the Digital SME Alliance according to SMEs' roles in the digital ecosystem are used. This categorization was proposed by the Digital SME Alliance in regard to addressing SME requirements in cybersecurity solutions and standards [i.2].

Third, the following five well-known cybersecurity standards and frameworks that can be used throughout the five-step process are introduced:

1) Cyber Essentials (UK).
2) The Centre for Cyber Security Belgium SME Guide (Belgium).
3) Center for Internet Security (CIS) Controls (USA), ETSI TR 103 305-1 [i.19] (Europe and global).
4) NIST Small Business Information Security (USA).
5) ISO/IEC 27002 [i.21] Code of practice for information security controls (International).

Fourth, a comparative analysis of these five cybersecurity standards and frameworks to provide a unified set of security controls is presented. The granularity of the controls differs in these standards and frameworks. However, by analysing them, 17 unified control categories that can be applied in organizations for reducing their cybersecurity risks are presented. The comparative analysis helps SMEs to be able to have a unified set of controls from different sources, and enables them to further focus on specific controls by easily referring to the controls in each of the standards and frameworks.

Fifth, the SME categories (Table 1) proposed by the Digital SME Alliance are further elaborated on [i.4]. Based on the implementation guidelines provided by CIS [i.5], guidance on how to use the comparative analysis and which controls might be applicable for different SME categories is presented. This enables SMEs to get tailored guidance for selecting controls with respect to their role in the digital ecosystem.

Finally, the way the five-step process and the five cybersecurity standards and frameworks can be used by SMEs is illustrated with an exemplar SME. This enables SMEs to understand the five-step process better.

Table 1: SME Categories according to their roles in the digital ecosystem [i.2]

SME Category	Description
Digital enablers	SMEs that are active in developing and providing cybersecurity solutions.
Digitally based	SMEs that are highly dependent on digital solutions for their business.
Digitally dependent	SMEs that depend on digital solutions as end users.
Start-ups	SMEs that neglect or are not well aware of cybersecurity and require specific measures and incentives to adopt cybersecurity solutions.

The annexes are presented for those looking for more information and organized as follows:

- Annex A: SME Standardization and the European Landscape.
- Annex B: Starting with Standards and Standardization.
- Annex C: Standards Developing Organizations.
- Annex D: Maturity Models for Cybersecurity and Information Security.

1 Scope

The present document provides SMEs with the main concepts of cybersecurity and introduces a five-step process for establishing cybersecurity using standards and frameworks in language that is easy for SMEs to understand. Five widely used standards and frameworks for SMEs from different countries and sources for reducing cybersecurity risks are introduced. The security controls present in these standards and frameworks are compared and unified in 17 control categories to provide SMEs with a quick reference. Since cybersecurity is closely associated with the roles of the SMEs in the digital ecosystem, four different SME categories are discussed (digital enablers, digitally based, digitally dependent, and start-ups) and SMEs are provided with tailored guidance on the implementation of the controls. Although the selection of controls should be based on the risks that are specific to the organization, the basic controls that are applicable to almost every organization can also be considered for direct implementation. The present document uses a holistic approach by integrating the main concepts, processes, security controls derived from the standards and frameworks, and a focus on different SME categories to present the cybersecurity essentials for SMEs.

Although the present document aims for providing SMEs anywhere in the world with cybersecurity standardization essentials, additional information relevant to European SMEs is provided in Annex A.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] B. Y. Ozkan and M. Spruit: "Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda", International Journal of Standardization Research (IJSR), Jul. 01, 2019.

NOTE: Available at www.igi-global.com/article/cybersecurity-standardisation-for-smes/253856.

[i.2] The European Digital SME Alliance, Brussels (Jan. 2020): "The EU Cybersecurity Act and the Role of Standards for SMEs".

NOTE: Available at https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf.

[i.3] ISO/IEC 27032:2012: "Information technology -- Security techniques -- Guidelines for cybersecurity".

NOTE: Available at https://www.iso.org/standard/44375.html.

[i.4] ISO/IEC 27000:2018: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

NOTE: Available at https://www.iso.org/standard/73906.html.

[i.5] World Economic Forum: "The Global Risks Report 2020".

NOTE: Available at https://wef.ch/2QfEAR9.

[i.6] C. H. Gañán, M. Ciere, and M. van Eeten: "Beyond the pretty penny: the Economic Impact of Cybercrime" in Proceedings of the 2017 New Security Paradigms Workshop, Santa Cruz, CA, USA, 2017, pp. 35-45, doi: 10.1145/3171533.3171535.

[i.7] C. P. Pfleeger, S. L. Pfleeger, and J. Margulies: "Security in computing", Fifth edition. Upper Saddle River, NJ: Prentice Hall, 2015.

[i.8] ISO/IEC 27001:2013: "Information technology -- Security techniques -- Information security management systems -- Requirements".

NOTE: Available at https://www.iso.org/standard/54534.html.

[i.9] European Commission: "The EU cybersecurity certification framework, Shaping Europe's digital future".

NOTE: Available at https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework.

[i.10] European Commission, 2018: "Cybersecurity Act".

NOTE: Available at https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en.

[i.11] ENISA 2020: "Standardisation in support of the Cybersecurity Certification".

NOTE: Available at https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i.

[i.12] ISO/IEC 27005:2018: "Information security risk management".

NOTE: Available at https://www.iso.org/standard/75281.html.

[i.13] ISO 31000:2018: "Risk management -- Guidelines".

NOTE: Available at https://www.iso.org/standard/65694.html.

[i.14] J. J. Cebula, M. E. Popeck, and L. R. Young: "A Taxonomy of Operational Cyber Security Risks Version 2", Defense Technical Information Center, Fort Belvoir, VA, May 2014. doi: 10.21236/ADA609863.

[i.15] L. Marinos: "ENISA Threat Taxonomy", 2016.

NOTE: Available at https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view.

[i.16] Center for Internet Security Mar. 2018: "CIS Controls V7 Measures & Metrics".

NOTE: Available at https://www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics/.

[i.17] NCSC (2020): "About Cyber Essentials".

NOTE: Available at https://www.ncsc.gov.uk/cyberessentials/overview.

[i.18] Centre for Cyber security Belgium, Jan. 20, 2017: "Guide for SME".

NOTE: Available at https://ccb.belgium.be/en/document/guide-sme.

[i.19] ETSI TR 103 305-1: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 1: The Critical Security Controls".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103300_103399/10330501/03.01.01_60/tr_10330501v030101p.pdf.

[i.20] C. Paulsen and P. Toth: "Small Business Information Security: The Fundamentals' National Institute of Standards and Technology", NIST Internal or Interagency Report (NISTIR) 7621 Rev. 1, Nov. 2016. doi: https://doi.org/10.6028/NIST.IR.7621r1.

[i.21] ISO/IEC 27002:2013: "Information technology -- Security techniques -- Code of practice for information security controls".

NOTE: Available at https://www.iso.org/standard/54533.html.

[i.22] Center for Internet Security, Jul. 2019: "CIS Controls and Sub-Controls Mapping to ISO 27001".

NOTE: Available at https://www.cisecurity.org/white-papers/cis-controls-and-sub-controls-mapping-to-iso-27001/.

[i.23] OWASP Foundation, 2020: "Denial of Service Software Attack".

NOTE: Available at https://owasp.org/www-community/attacks/Denial_of_Service.

[i.24] European Commission, COM (2016) 176 final, Apr. 19, 2016: "ICT Standardisation Priorities for the Digital Single Market".

NOTE: Available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0176&from=EN.

[i.25] European Commission, 2020: "2020 Rolling Plan for ICT Standardisation".

NOTE: Available at https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2020.

[i.26] CEN-CENELEC, July 11, 2019: "SME Standardization Toolkit (SMEST 2)".

NOTE Available at https://www.cencenelec.eu/sme/SMEST/Pages/default.aspx.

[i.27] CEN-CENELEC, May 06, 2021: "SME Toolbox of Solutions".

NOTE: Available at https://www.cencenelec.eu/sme/std/Pages/default.aspx.

[i.28] ETSI white paper n 6 (Febuary 2011): "Participation of SMEs in Standardization".

NOTE: Available at https://www.etsi.org/images/files/ETSIWhitePapers/WP_No_6_SME_FINAL.pdf.

[i.29] The European Digital SME Alliance, Feb. 07, 2020: "Standardisation Success Story: Relevance to SMEs becomes a priority for new ETSI standards".

NOTE: Available at https://www.digitalsme.eu/relevance-to-smes-becomes-a-priority-for-new-etsi-standards/ (accessed March 06, 2020).

[i.30] Small Business Standards (SBS) (November 2016): "Small Business Standards User Guide for European SMEs on ISO 26000 Guidance on Social Responsibility", Accessed: Nov. 13, 2019.

NOTE: Available at https://www.sbs-sme.eu/sites/default/files/publications/SBS%20SME%20ISO%20User%20Guide%202016_FINAL.pdf.

[i.31] Small Business Standards (SBS) (2018), Digital SME Alliance: "SME Guide for the implementation of ISO/IEC 27001 on information security management", Accessed: Sep. 02, 2018.

NOTE: Available at https://www.digitalsme.eu/digital/uploads/SME-Guide-for-the-implementation-of-ISOIEC-27001-on-information-security-management.pdf.

[i.32] European Network and Information Security Agency: "Guidelines for SMEs on the security of personal data processing", ENISA, 2016.

[i.33] M. Dekker, D. Liveri, Europäische Union, and Agentur für Netz- und Informationssicherheit, Cloud security guide for SMEs cloud computing security risks and opportunities for SMEs. Heraklion, 2015.

[i.34] C. G. Manso, E. Rekleitis, F. Papazafeiropoulos, and V. Maritsas: "Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises". Heraklion: ENISA, 2015.

[i.35] ECSO (2019): "European Cyber Security Organisation - Work Group 4".

NOTE: Available at https://ecs-org.eu/working-groups/wg4-support-to-smes-coordination-with-countries-and-regions.

[i.36] ECSO (2019): "European Cyber Security Organisation - Work Group 1".

NOTE: Available at https://ecs-org.eu/working-groups/wg1-standardisation-certification-and-supply-chain-management.

[i.37] ECSO (2017): "ECSO State of the Art Syllabus v2".

NOTE: Available at http://www.ecs-org.eu/documents/uploads/updated-sota.pdf.

[i.38] ISO, May 14, 2019: "Standards".

NOTE: Available at http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards.html.

[i.39] ISO, 2019: "Benefits of standards".

NOTE: Available at http://www.iso.org/cms/render/live/en/sites/isoorg/home/standards/benefits-of-standards.html.

[i.40] ISO: "ISO and Small & Medium Enterprises".

NOTE: Available at https://www.iso.org/iso-and-smes.html.

[i.41] StandICT.eu, 2020: "The European Observatory For ICT Standardisation".

NOTE: Available at https://www.standict.eu/euos.

[i.42] European Commission, July 05, 2016: "Internal Market, Industry, Entrepreneurship and SMEs - Standardisation and SMEs".

NOTE: Available at https://ec.europa.eu/growth/smes/access-to-markets/standardisation_en.

[i.43] CEN, 2020: "CEN - CEN Community - Members - List of members".

NOTE: Available at https://standards.cen.eu/dyn/www/f?p=CENWEB:5.

[i.44] P. B. Crosby: "Quality is Free: The Art of Making Quality Certain". McGraw-Hill, 1979.

[i.45] M. C. Paulk, B. Curtis, M. B. Chrissis, and C. V. Weber: "Capability Maturity Model, Version 1.1", IEEE Software; Los Alamitos, vol. 10, no. 4, pp. 18-27, 1993.

NOTE: Available at http://dx.doi.org/10.1109/52.219617.

[i.46] N. T. Le and D. B. Hoang: "Can maturity models support cyber security?", in 2016 IEEE 35th International Performance Computing and Communications Conference (IPCCC), December 2016, pp. 1-7, doi: 10.1109/PCCC.2016.7820663.

[i.47] US Department of Energy, 2014: "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)".

NOTE: Available at https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf.

[i.48] The Open Group, 2017: "Open Information Security Management Maturity Model (O-ISM3), Version 2.0".

NOTE: Available at https://publications.opengroup.org/c17b.

[i.49] US Department of Homeland Security, Aug. 04, 2014: "National Initiative for Cybersecurity Education - Cybersecurity Capability Maturity Model White Paper".

NOTE: Available at https://www.hsdl.org/?view&did=798503.

[i.50] Marco Spruit and Martijn Roeling: "ISFAM: The Information Security Focus Area Maturity Model", in Proceedings of the European Conference on Information Systems (ECIS) 2014, June 9-11, 2014, Tel Aviv, Israel, June 2014, p. 15.

NOTE: Available at https://aisel.aisnet.org/ecis2014/proceedings/track14/6.

[i.51] IASME Consortium: "Cyber Essentials Self-Assessment Preparation Booklet".

NOTE: Available at https://iasme.co.uk/wp-content/uploads/2020/03/Cyber-Essentials-only-question-booklet-v11b.pdf.

[i.52] ISO/IEC/IEEE 15939:2017: "Systems and software engineering -- Measurement process".

NOTE: Available at https://www.iso.org/standard/71197.html.

[i.53] ISO/IEC 27033-1:2015: "Information technology -- Security techniques -- Network security -- Part 1:Overview and concepts".

NOTE: Available at https://www.iso.org/standard/63461.html.

[i.54] ISO/IEC 27034-1:2011: "Information technology -- Security techniques -- Application security -- Part 1: Overview and concepts".

NOTE: Available at https://www.iso.org/standard/44378.html.

[i.55] ISO/IEC 27035-1:2016: "Information technology -- Security techniques -- Information security incident management -- Part 1: Principles of incident management".

NOTE: Available at https://www.iso.org/standard/60803.html.

[i.56] ISO 22301:2019: "Security and resilience -- Business continuity management systems -- Requirements".

NOTE: Available at https://www.iso.org/standard/75106.html.

[i.57] ISO/IEC 27036-1:2014: "Information technology -- Security techniques -- Information security for supplier relationships -- Part 1: Overview and concepts".

NOTE: Available at https://www.iso.org/standard/59648.html.

[i.58] ETSI TR 103 305-4: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 4: Facilitation Mechanisms".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103300_103399/10330504/02.01.01_60/tr_10330504v020101p.pdf.

[i.59] Center for Internet Security, Sept. 2017: "CIS Controls Implementation Guide for Small- and Medium-Sized Enterprises (SMEs)".

NOTE: Available at https://www.cisecurity.org/wp-content/uploads/2017/09/CIS-Controls-Guide-for-SMEs.pdf.

[i.60] Center for Internet Security, April 2018: "CIS Risk Assessment Method".

NOTE: Available at https://learn.cisecurity.org/cis-ram.

[i.61] ISO/IEC 27004: "Information technology -- Security techniques -- Information security management -- Monitoring, measurement, analysis and evaluation".

NOTE: Available at https://www.iso.org/standard/64120.html.

[i.62] ETSI TR 103 305-2: "CYBER; Critical Security Controls for Effective Cyber Defence; Part 2: Measurement and auditing".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

availability: property of being accessible and usable on demand by an authorized entity

NOTE: See ISO/IEC 27000:2018 [i.4].

confidentiality: property that information is not made available or disclosed to unauthorized individuals, entities, or processes

NOTE: See ISO/IEC 27000:2018 [i.4].

integrity: property of accuracy and completeness

NOTE: See ISO/IEC 27000:2018 [i.4].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

BSI	British Standards Institutuion
CEN	Comite Europeen de Normalisation (European Committee for Standardisation)
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIA	Confidentiality (C), Integrity (I) and Availability (A)
CIS	Center for Internet Security
CMM	Capability Maturity Model
DDoS	Distributed Denial of Service
DOE	Department Of Energy
DoS	Denial of Service
EC	European Commission
ECSO	European Cyber Security Organisation
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
HR	Human Resources
IASME	Information Assurance Small and Medium-sized Enterprises
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
IG	Implementation Group
IoT	Internet of Things
ISFAM	The Information Security Focus Area Maturity Model
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
NEN	Royal Netherlands Standardization Institute
NCSC	National Cyber Security Centre
NICE	National Initiative for Cybersecurity Education
NIST	The National Institute of Standards and Technology (USA)
OWASP	Open Web Application Security Project
PCI	Payment Card Industry
RAM	Risk Assessment Method
SBS	Small Business Standards

SDOs	Standards Developing Organizations
SFs	Standards and Frameworks
SME	Small and Medium Sized Enterprise
UPS	Uninterruptible Power Supplies
WG	Working Group

4 Background: What SMEs Need to Know About Cybersecurity?

In this clause, firstly, the position of cybersecurity and information security with respect to the other disciplines in the security domain is presented. Secondly, the main objectives of cybersecurity and information security are described. Thirdly, the concepts of threat, control and risk which are important to better understand what could cause harm to security are introduced.

The domains of information security and cybersecurity are quite intertwined. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have been developing and publishing many international standards, including the ISO/IEC 27032 [i.3] guideline for cybersecurity. ISO/IEC 27032 [i.3] standard presents the relationships between cybersecurity, information security and other security domains as shown in Figure 1.

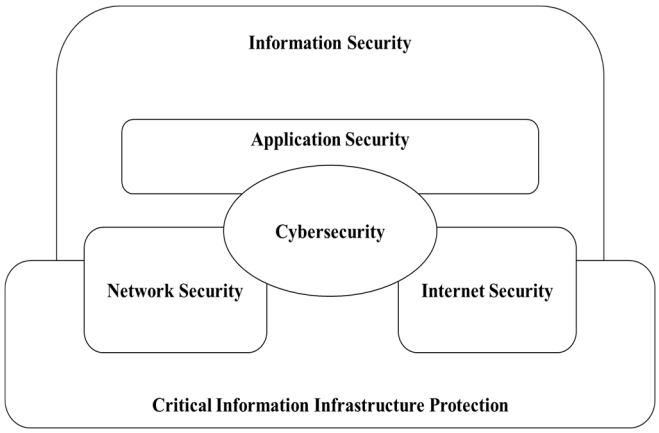


Figure 1: Relationships between cybersecurity and other security domains (redrawn from ISO/IEC 27032 with the copyright permission of NEN, Delft, www.nen.nl) [i.3])

The ISO/IEC 27032 standard [i.3] defines the relationship between cybersecurity and other security domains as follows. Cybersecurity relies on information security, application security, network security, and Internet security as fundamental building blocks. It has a unique scope requiring stakeholders to play an active role in order to maintain, if not improve the usefulness and trustworthiness of the Cyberspace.

A basic definition of cybersecurity is "*preservation of confidentiality, integrity and availability of information in the Cyberspace*" and a basic definition of information security is "*preservation of confidentiality, integrity and availability of information*" as per ISO/IEC 27000 [i.4]. These definitions bring to the three main objectives of cybersecurity and information security: Confidentiality (C), Integrity (I) and Availability (A). These three objectives (also known as the CIA triad) are defined in clause 3.1 and depicted in Figure 2. It is deemed important to know these concepts for any organization since the principle for establishing security is to make sure these aspects of organizational information are protected.

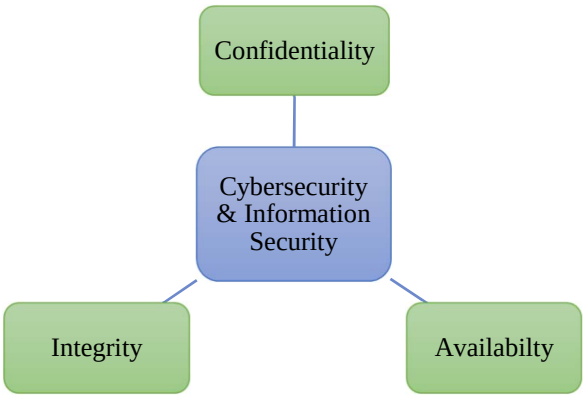


Figure 2: Confidentiality, Integrity and Availability (CIA Triad)

The World Economic Forum publishes annual global risk reports. The 2020 report revealed that cyberattacks are in the 7th and 8th place in the Top 10 risks with respect to the likelihood and impact, respectively. In 2021, cybercrime damages are estimated to reach US$ 6 trillion [i.5]. Cyberattacks have both short term and long term economic impacts in terms of losses and expenses [i.6].

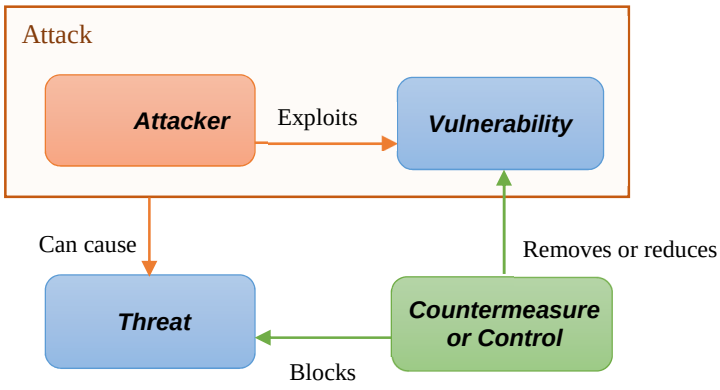


Figure 3: Threat-Vulnerability-Control Paradigm based on [i.7]

Cybersecurity and information security are all about risk management. Every company has valuable assets to protect (to protect the CIA of these assets) and assets might have different vulnerabilities contributing to different risks. Since not all risks can be eliminated, the organizations need to decide what risks they can accept and what risks they need to mitigate. The cybersecurity and information security risks that an organization faces are associated with its operating environment (both external and internal), and the measures should be driven by the needs and expectations of interested parties.

These vulnerabilities of the assets might be exploited by threats. This might cause a risk. Countermeasures (i.e. controls) should be implemented to mitigate the risks.

EXAMPLE: An organization can have a web server (ASSET) which is crucial to its business. There could be cyber-attacks (ATTACK) such as a Denial of Service (DoS) targeted to this web server. If the webserver does not have the latest security patches (VULNERABILITY), the attacker can exploit this vulnerability causing a threat to the organization. The probability of this scenario happening and the impact of it on the organization constitutes the risk. The organization has options to reduce or remove the vulnerability of the webserver by applying the latest security patches. Another option might be detecting and blocking the DoS attack. Figure 3 illustrates the relationships between a threat, a vulnerability and a control.

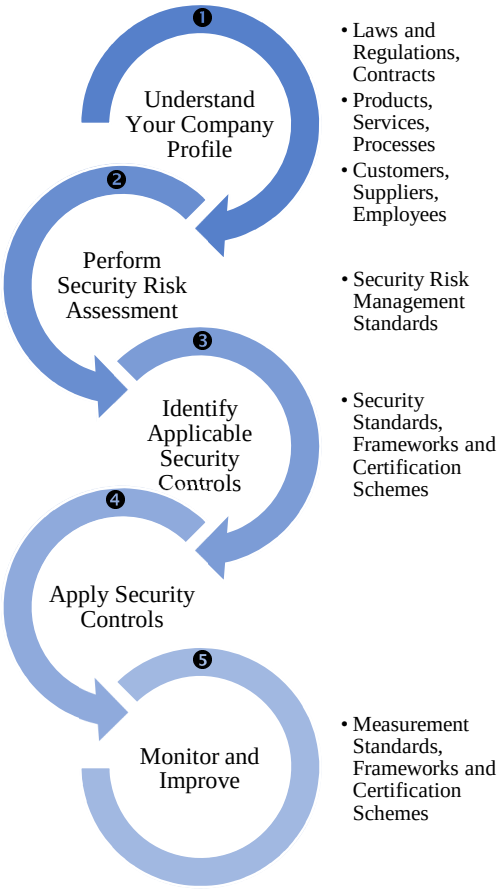
5 The Five-Step Process to Establish and Improve Cybersecurity for SMEs

5.1 Introduction

The five-step process for establishing and improving cybersecurity in an organization by using frameworks, standards and certification schemes is depicted in Figure 4. These steps are derived from the ISO/IEC 27001 [i.8] standard's Planning clause. To understand the five-step process better, the reader is encouraged to check the illustrative example in the clause 8 "Exemplary Application".

This five-step process should be considered as the beginning of a long and never-ending journey. New vulnerabilities and threats will always exist given the ever-changing technologies. The aim of the monitor and improve step is to ensure the adaptation of the organizations to emerging security requirements.

Clauses 5.2 to 5.6 describe the process steps in detail.



NOTE: There are more steps in this standard clause to fulfil all the requirements of an Information Security Management System (ISMS). Here, the process is simplified for starting a quick implementation to use standards for establishing information security (or cybersecurity).

Figure 4: The basic process for establishing and improving cybersecurity by using frameworks, standards and certification schemes (based on the Planning clause of the ISO/IEC 27001 [i.8])

5.2 (Step 1) Understand Your Company Profile

The first step is about understanding the organization and its context. The internal and external issues play a role in understanding the context of the organization and its ability to establish and improve cybersecurity. This step is directly related to the Context of the organization clause of the ISO/IEC 27001 [i.8].

The following questions can help to understand the internal and external issues:

- How is our organizational structure? What are the main roles in the organization?
- What products and services do we provide?
- What processes do we have?
- What regulatory and contractual obligations do we have?
- What are our objectives?
- What resources do we have? (Including employees, systems, equipment, etc.)
- Who are our customers and suppliers?
- Who are the interested parties for our cybersecurity efforts?
- What are the needs and expectations of these parties?

In the following paragraphs, resources that aim to address different SMEs according to their organizational context are provided.

In case the organization provides products and/or services, the SME needs to ensure that its products and services meet the security requirements. These security requirements may stem from cybersecurity certification schemes. The EU Cybersecurity Act creates a framework [i.9] for European Cybersecurity Certificates for products, processes and services that is valid throughout the EU [i.10]. An ENISA publication elaborates on standards and the role of Standards Developing Organizations (SDOs) in cybersecurity certification [i.11].

Steps 2, 3, and 4 of the five-step process are part of the risk management process. ISO/IEC 27005 [i.12] specifically addresses information security risk management. There is also a more generic risk management standard published by ISO which is ISO 31000 [i.13]. ISO/IEC 27000 [i.4] defines the risk management process as "*the systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context and identifying, analysing, evaluating, treating, monitoring and reviewing risk*". A generic risk management process is depicted in Figure 5.

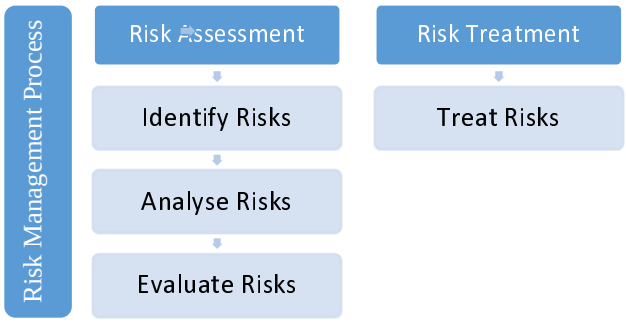


Figure 5: Risk Management Process (based on the Planning clause of ISO/IEC 27001 [i.8])

5.3 (Step 2) Perform Security Risk Assessment

The risk assessment process should follow predefined, repeatable and traceable steps. At this stage, risk acceptance criteria should be identified including the regulatory and contractual requirements and business objectives.

Step 1 - Identify Risks: In this step, the organization should consider its assets (any item valuable to the organization), the vulnerabilities of these assets and the likelihood of possible threats. The value of the assets is associated with the way they are used by the business.

EXAMPLE: for an organization providing e-commerce services to its customers, the computers hosting the e-commerce application are critical assets.

Risk owners should be assigned at this stage. Cyber security risk taxonomies (i.e. [i.14]), threat taxonomies (i.e. [i.15]) and risk reports (i.e. [i.5]) can help organizations identifying their risks.

Step 2 - Analyse Risks: This step involves assessing the potential impact and realistic probability of the occurrence of the risks. Risk level is determined based on the impact and the probability of the risk. Risk level can be formulated as a function of impact and probability of a security event as follows:

$$R = f(impact \times probability)$$

The impact of a loss of confidentiality, integrity and availability should all be considered. The risk can be quantified using the designated impact and probability.

Step 3 - Evaluate Risks: The quantified risks should be compared against the pre-set risk acceptance criteria and prioritized by their level for risk treatment.

In ETSI TR 103 305-4 [i.58], clause 7 is about risk assessment method and refers to the CIS Risk Assessment Method (RAM) document [i.60]. SMEs can find further guidance in the CIS RAM for performing this step of the five-step process.

5.4 (Step 3) Identify Applicable Security Controls (Risk Treatment)

Risk treatment is a step in the risk management process (see Figure 5). According to ISO/IEC 27000 [i.4], possible options for risk treatment include:

1) reducing the risks by applying controls;

2) accepting risks according to the risk acceptance criteria;

3) avoiding risks by not allowing actions that would cause the risks to occur; and

4) sharing the risks to other parties such as insurers (i.e. cyber insurers) or suppliers.

If the organization decides the first option (reducing the risks), controls (i.e. countermeasures) need to be selected and implemented.

In the present document a comparative analysis of five well-known standards and frameworks for cybersecurity controls from different countries and sources is presented to provide a quick reference of control categories (17 in total) for SMEs (see Table 2). To identify the applicable controls, at this step, SMEs are encouraged to refer to clause 7 "Four Categories of SMEs in Cybersecurity Context" to identify the category of their company regarding its role in the digital ecosystem. In the aforementioned clause, guidance to identify applicable controls per SME category is provided.

There are three types of controls:

- physical controls (locks, access-controlled rooms, security guards, etc.);
- procedural or administrative controls (laws, regulations, policies, contracts, agreements, operational procedures, trainings etc.); and
- technical controls (firewalls, encryption, malware protection programs, etc.) [i.7].

As described in the previous section, a comparative analysis of 17 control categories from different standards and frameworks are introduced in Table 2. In Table 3, these control categories and the control types they comprise are listed. SMEs can use this table for planning the resources required for implementing the selected controls. The application of the technical controls requires technical or security knowledge and expertise. The procedural and physical controls are most likely to be implemented with the available resources.

5.5 (Step 4) Apply Security Controls (Risk Treatment)

An implementation plan can be prepared for the application of identified security controls at the organization. The CEO can prepare such an implementation plan or they can delegate this to someone in the organization. The prioritization of the tasks should be aligned with the prioritization of the associated risks. There should be people responsible for the implementation of selected controls who are capable in terms of time and knowledge. SMEs might not have the necessary resources to implement the technical controls. In this case, using services from consultancy firms should be considered.

5.6 (Step 5) Monitor and Improve

The identified risks should be monitored and reviewed regularly (at least annually). Reviews should be carried out after any change in the organization that may affect the risks. The necessary risk management steps should be conducted again if required.

To ensure that the security controls are functioning as expected, they need to be monitored and reviewed. This step also contributes to the overall evaluation and improvement efforts to establish cybersecurity. There are several standards that can help in monitoring and improving the controls that are chosen to be applied.

ISO/IEC 27004 [i.61] explains how to develop and operate measurement processes, and how to assess and report the results of a set of information security metrics. The Center for Internet Security (CIS) Controls Measures and Metrics document presents a list of measures for each control that can be used to monitor and improve the applied controls [i.16]. Although the ISO/IEC/IEEE 15939 [i.52] standard is focused on systems and software engineering, it provides a generic framework on how to establish a measurement process in an organization.

Apart from the monitor and improve step, process evaluations, certification and compliance audits are some of the other tools to ensure that the security controls are functioning as expected and the risk management processes are effective.

6 Five Cybersecurity Frameworks and Standards for SMEs and their Comparative Analysis

6.1 Introduction

In this clause, five different frameworks and standards are introduced. These frameworks and standards provide organizations (some of them specifically focus on SMEs) with security controls that could be applied for risk treatment. The decision of selecting controls to apply should normally be based on the results of risk assessment of the organizations. Some of the standards and frameworks that are presented below include a number of controls that could be applied even before a comprehensive risk assessment. The aim of providing organizations with such a basic set of controls is to support them against the basic threats that they could face. Applying additional controls should be a cost/benefit analysis decision that should be taken by the organization given their limited resources (especially for start-ups). The standards and frameworks (SFs) will be referred in the given order as SF1, SF2 and so on.

SF1 - Cyber Essentials *(UK)* is a cybersecurity scheme backed by the UK government and operated by National Cyber Security Centre (NCSC) of the UK government. Cyber Essentials provides organizations with a set of fundamental controls against threats coming from the internet [i.17].

Cyber Essentials includes two levels of certification as follows. In Cyber Essentials scheme, organizations perform self-assessment against five basic security controls and a qualified assessor verifies the information provided. In the Cyber Essentials Plus scheme, a qualified assessor examines the same controls, testing that they work through a technical audit. To learn more about certification, the IASME consortium website can be visited (https://iasme.co.uk/). The latest self-assessment preparation questionnaire can also be downloaded [i.51].

SF2 - The Centre for Cyber Security Belgium SME Guide *(Belgium)* was developed by the Centre for Cyber Security Belgium in partnership with the Cyber Security Coalition Belgium for small and medium-sized enterprises [i.18]. It is based on input and best practices from private and public entities [i.18]. SMEs can use the list of 12 cyber security topics with basic and advanced cybersecurity recommendations against data breaches and cyber-attacks. The SME guide is freely accessible online [i.18].

SF3 - Center for Internet Security (CIS) Controls (USA) and ETSI TR 103 305-1 [i.19] *(Europe & global))* are published by CIS and ETSI, respectively. The Center for Internet Security (CIS) is a non-profit organization based in United States with members including large corporations, government agencies, and academic institutions. The latest version of CIS Controls is freely accessible online [i.16].

In version 7.1 of the CIS Controls, based on the following three characteristics, three Implementation Groups (IGs) are defined:

- Data sensitivity and criticality of services offered by the organization.
- Expected level of technical expertise exhibited by staff or on contract.
- Resources available and dedicated toward cybersecurity activities.

The implementation groups are defined as IG 1, IG 2 and IG 3. The following could be considered as examples of organizations in these IGs.

- *IG 1:* An IG 1 organization is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. This group corresponds to the Start-ups SMEs in Table 1.
- *IG 2*: An IG 2 organization employs individuals responsible for managing and protecting IT infrastructure. This group corresponds to the Digital Dependent SMEs in Table 1.
- *IG 3:* An IG 3 organization employs security experts that specialize in the different facets of cybersecurity (e.g. risk management, penetration testing, and application security). This group corresponds to both the Digital Enabler and Digitally Based SMEs in Table 1.

Even though this IG approach provides guidance for prioritizing usage of the CIS Controls, CIS advises that organizations should better base their decisions on their organisation's risk assessment. CIS includes 20 controls and 171 sub-controls. The assignment of controls to IGs is done at the sub-control level. IG 1 includes the minimum set of sub-controls. IG2 has additional sub-controls for IG 2 and the same is valid for IG 3 that includes the full set of 171 sub-controls.

ETSI has published technical report ETSI TR 103 305-1 [i.19] that is technically equivalent and compatible with CIS Controls, Version 7.0 of the Center for Internet Cybersecurity. In ETSI TR 103 305-4 [i.58], there is guidance for SMEs that refers to CIS's implementation guide for SMEs [i.59]. This guide is considered suitable for the Start-ups SMEs in Table 1 as it contains a small sub-set of the Controls specifically selected to help protect SMEs.

SF4 - NIST Small Business Information Security *(USA)* is published by the National Institute of Standards and Technology (NIST) of the USA as a cybersecurity reference guideline for small businesses. The aim of the guideline is to help SMEs establishing and improving cybersecurity in non-technical language which is freely accessible [i.20]. In this guide recommendations are organized by the five Cybersecurity Framework Core Functions (Identify, Protect, Detect, Respond and Recover). There are 20 recommended actions in total under these categories. In addition, the guide provides 9 other recommendations towards users and employees. This guidance also includes some worksheets to help SMEs on how to conduct risk assessment. Sample policy and procedures statements are also provided in the appendices.

SF5 - ISO/IEC 27002 [i.21] Code of Practice for Information Security Controls *(International)* provides best practice recommendations on information security controls for initiating, implementing or maintaining Information Security Management Systems (ISMS) taking into consideration the organization's information security risk environment(s).

ISO/IEC 27001 [i.8] defines the requirements for an Information security management system. In Annex A of this standard, reference control objectives and controls are listed that could be applied to reduce information security risks. ISO/IEC 27002 [i.21] provides detailed guidelines for implementing these controls. There are 114 controls in 14 clauses included in ISO/IEC 27002 [i.21].

6.2 Standards and Frameworks for Security Controls - A Comparative Analysis

In this clause, a comparative analysis of the five standards and frameworks presented above is given (Table 2). It should be noted that physical and environmental controls are listed in this analysis only for the Incident and Continuity Management controls. Although, as part of the ISO/IEC 27002 standard [i.21], physical and environmental controls have 15 sub-controls, the other four standards do not include corresponding controls. This is because physical and environmental controls are not considered as part of cybersecurity. In the last column of Table 2, "Additional Standards to Consider" are presented. These standards are the specific standards that address the associated controls in detail. The ISO/IEC 27000 [i.4] series of standards include specific standards that address some of the controls elaborately. All of the standards in this series can be accessed on ISO's standards search webpage (https://www.iso.org/search.html?q=27000&hPP=10&idx=all_en&p=0&hFR%5Bcategory%5D%5B0%5D=standard).

The following are some examples of those specific standards:

- ISO/IEC 27033-1 [i.53] provides detailed guidance on implementing the network security controls that are introduced in ISO/IEC 27002 [i.21] (Category: 13 Communications security that includes 7 controls).
- ISO/IEC 27034-1 [i.54] focuses on application security and provides detailed guidance on implementing system acquisition, development and maintenance controls that are introduced in ISO/IEC 27002 [i.21] (Category: 14 System acquisition, development and maintenance that includes 13 controls).
- ISO/IEC 27035-1 [i.55] provides detailed guidance on implementing information security incident management controls that are introduced in ISO/IEC 27002 [i.21] (Category: 16 Information security incident management that includes 7 controls).
- ISO 22301 [i.56] provides detailed guidance on establishing business continuity management systems while the information security aspects of business continuity management are addressed in ISO/IEC 27002 [i.21] (Category: 17 Information security aspects of business continuity management that includes 4 controls).
- ISO/IEC 27036-1 [i.57] provides detailed guidance on implementing information security for supplier relationships controls that are introduced in ISO/IEC 27002 [i.21] (Category: 15 Supplier relationships that includes 5 controls).

Table 2: Standards and frameworks for security controls - a comparative analysis

#	*Control Category*	*[1] Cyber Essentials (UK)*	*[2] The Centre For Cyber Security Belgium SME Guide (Belgium)*	*[3] Center for Internet Security (CIS) (USA) + ETSI TR 103 305-1 [i.19] (Europe)*	*[4] NIST Small Business Information Security (USA)*	*[5] ISO/IEC 27002 [i.21] Code of Practice for Information Security Controls*	*Additional Standards to Consider*
1	Management commitment and policies		• Involving Top Management • Publish a Corporate Security Policy and a Code of Conduct		• Create policies and procedures for information security	6 Organizing information security 5 Information security policies	
2	Asset Management		• Manage Your Key ICT Assets	• Inventory and Control of Hardware Assets • Inventory and Control of Software Assets	• Identify what information your business stores and uses • Determine the value of your information • Develop an inventory • Dispose of old computers and media safely	8 Asset management	
3	Patch Management	• Patch Management	• Update All Programs	• Continuous Vulnerability Management	• Patch your operating systems and applications	12 Operations security	
4	Access Control	• Access Control	• Manage Access To Your Computers And Networks	• Controlled Use of Administrative Privileges • Controlled Access Based on the Need to Know • Account Monitoring and Control	• Use strong passwords • Limit employee access to data and information • Identify and control who has access to your business information • Require individual user accounts for each employee	9 Access control	
5	Secure Computers, Servers and Network Configuration	• Secure Configuration	• Secure Workstations and Mobile Devices • Secure Servers and Network Components	• Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	• Use separate personal and business computers, mobile devices, and accounts • Do not connect personal or untrusted storage devices or hardware into your computer, mobile device, or network	12 Operations security 13 Communications security	
6	Log Management			• Maintenance, Monitoring and Analysis of Audit Logs	• Maintain and monitor logs	12 Operations security	

#	Control Category	[1] Cyber Essentials (UK)	[2] The Centre For Cyber Security Belgium SME Guide (Belgium)	[3] Center for Internet Security (CIS) (USA) + ETSI TR 103 305-1 [i.19] (Europe)	[4] NIST Small Business Information Security (USA)	[5] ISO/IEC 27002 [i.21] Code of Practice for Information Security Controls	Additional Standards to Consider
7	Email and Web Security			• Email and Web Browser Protections	• Set up web and email filters • Be careful downloading software • Watch for harmful pop-ups • Be careful of email attachments and web links • Conduct online business more securely	12 Operations security	
8	Malware Protection	• Malware Protection	• Install Antivirus Protection	• Malware Defenses	• Install and update anti-virus, -spyware, and other malware programs	12 Operations security	
9	Network and Communications Security	• Boundary firewalls	• Secure Servers And Network Components • Secure Remote Access	• Limitation and Control of Network Ports, Protocols, and Services • Secure Configuration for Network Devices, such as Firewalls, Routers and Switches • Boundary Defense • Wireless Access Control • Penetration Tests and Red Team Exercises	• Install and activate software and hardware firewalls on all your business networks • Secure your wireless access point and networks	13 Communications security	• ISO/IEC 27033-1 [i.53] - Network security
10	Back-up and Recovery Management		• Backup All Information	• Data Recovery Capabilities	• Make full backups of important business data/information • Make incremental backups of important business data/information	12 Operations security	
11	Data Protection and Encryption			• Data Protection	• Use encryption for sensitive business information	10 Cryptography 18 Compliance	
12	Awareness and Training		• Raise Staff Awareness of Cyber Risks	• Implement a Security Awareness and Training Program	• Train your employees • Do not give out personal or business information	7 Human resource security	
13	Secure Development			• Application Software Security		14 System acquisition, development and maintenance	• ISO/IEC 27034-1 [i.54]: Application security, OWASP Top 10, PSI Security Standards

#	Control Category	[1] Cyber Essentials (UK)	[2] The Centre For Cyber Security Belgium SME Guide (Belgium)	[3] Center for Internet Security (CIS) (USA) + ETSI TR 103 305-1 [i.19] (Europe)	[4] NIST Small Business Information Security (USA)	[5] ISO/IEC 27002 [i.21] Code of Practice for Information Security Controls	Additional Standards to Consider
14	Incident and Continuity Management		• Have a Business Continuity and an Incident Handling Plan	• Incident Response and Management	• Install Surge Protectors and Uninterruptible Power Supplies (UPS) • Develop a plan for disasters and information security incidents • Consider cyber insurance	11 Physical and environmental security 16 Information security incident management 17 Information security aspects of business continuity management	• SO/IEC 27032 [i.3]: Incident management • ISO 22301 [i.56]: Business continuity management
15	Human Resource Security				• Conduct Background Checks • Pay attention to the people you work with and around	7 Human resource security	
16	Improvement and Compliance				• Make improvements to processes / procedures / technologies	16 Information security incident management 18 Compliance	• ISO/IEC 27035-1 [i.55]: Incident management • ISO/IEC 27004 [i.61]: Measurement • ETSI TR 103 305-2 [i.62]: Measurement and auditing • ISO/IEC/IEEE 15939 [i.52]: Measurement process
17	Supplier Relationships					15 Supplier relationships	• ISO/IEC 27036-1 [i.57]: Information security for supplier relationships

In Table 3, the unified list of control categories is presented together with the types of controls they comprise. The types of controls are discussed in Step 4 of the five-step process in Figure 4.

Table 3: 17 Control categories from five standards and frameworks and the types of controls in the categories

#	Control Category	Procedural	Physical	Technical
1	Management commitment and policies	X		
2	Asset Management	X	X	X
3	Patch Management	X		X
4	Access Control	X	X	X
5	Secure Computers, Servers and Network Configuration	X	X	X
6	Log Management	X		X
7	Email and Web Security	X		X
8	Malware Protection	X		X
9	Network and Communications Security	X		X
10	Back-up and Recovery Management	X		X
11	Data Protection and Encryption	X	X	X
12	Awareness and Training	X		
13	Secure Development	X		X
14	Incident and Continuity Management	X	X	X
15	Human Resource Security	X	X	
16	Improvement and Compliance	X		X
17	Supplier Relationships	X	X	X

7 Four Categories of SMEs in Cybersecurity Context

As mentioned in the Introduction clause, the European Digital SME Alliance published their position paper on the EU Cybersecurity Act and the role of standards for SMEs [i.2]. In this clause, the four categories of SMEs within a cybersecurity context are further explained. ECSO's State of the Art Syllabus [i.37] presents an overview of cybersecurity standards categorized by industry, products, components and services that might be useful for all categories of SMEs.

Digital Enabler SMEs are less likely to face challenges in adopting cybersecurity standards. Since they develop or provide cybersecurity solutions, they might focus on the certification of their products and/or services. Apart from developing and providing cyber secure solutions, these types of SMEs should protect their assets. They need to consider the security of their processes and of their information. Intellectual Property Rights (IPR) should be another aspect to consider for these type of SMEs as they might be working on innovative cybersecurity solutions.

According to the Center for Internet Security (CIS) criteria presented in clause 6.1, Digital Enabler SMEs correspond to the CIS's Implementation Group 3 (IG 3). The services offered by Digital Enabler SMEs are critical for the security of other organizations as well. These SMEs should refer to IG 3 of the CIS Controls and expand their implementation with the comparative analysis that is provided in Table 2. There is also another document of the CIS that provides sub-control level mapping of CIS Controls to ISO 27001 [i.22] Annex 1 and therefore ISO/IEC 27002 controls [i.21].

Digitally Based SMEs depend on digital solutions to run their businesses, according to their domain of operation (e.g. health, finance, critical infrastructures, e-government). Therefore, they should be aware of related standards available and they need to adhere. According to the Center for Internet Security (CIS) criteria presented in clause 6.1, Digitally Based SMEs correspond to the Implementation Group 3 (IG 3). The business model of Digitally Based SMEs is dependent on digital solutions provided by their vendors. These SMEs should refer to IG 3 of the CIS Controls and expand their control implementation with the comparative analysis that is provided in Table 2. There is also another document of the CIS that provides sub-control level mapping of CIS Controls to ISO 27001 [i.22] Annex1 and therefore ISO/IEC 27002 [i.21] controls (CIS, 2019).

Digitally Dependent SMEs depend on ICT to run their businesses, according to their domain of operation (e.g. health, finance, critical infrastructures, e-government). Therefore, they should be aware of related standards available and they need to adhere. According to the Center for Internet Security (CIS) criteria presented in clause 6.1, Digitally Dependent SMEs correspond to the Implementation Group 2 (IG 2). The business model of Digital Dependent SMEs are dependent on ICT provided by their vendors. These SMEs should refer to IG 2 of the CIS Controls and expand their control implementation with the comparative analysis that is provided in Table 2.

Start-ups are defined as a sub-group of the first or second category [i.2]. Security has a low priority for the SMEs in this category. According to the alliance, this category of enterprises requires specific measures and incentives to adopt security standards. According to the Center for Internet Security (CIS) criteria presented in clause 6.1, Start-ups correspond to the Implementation Group 1 (IG 1). These SMEs should refer to IG 1 of the CIS Controls and expand their control implementation with the comparative analysis that is provided in Table 2.

8 Exemplary Application: Cybersecurity Essentials for SME "UP"

SMEs are encouraged to read the background information provided in the present document first to get familiar with the cybersecurity concepts. The next step is to follow the five-step process (Figure 4).

In this clause, an exemplar SME which will be referred to as "UP" is considered to present some tips on how to use the recommended five-step process presented in Figure 4. The exemplar SME is used to help the reader better understand the provided cybersecurity essentials in a more actionable manner.

Our exemplar SME, UP, has a main business of providing an online platform for e-trainings. The Chief Executive Officer (CEO) of the SME has read the annual risk reports (i.e. [i.5]) and was concerned about the security of its organization and its online platform. They then read the present document. After understanding some basic terminology about cybersecurity (see Introduction), they follow the steps presented in Figure 4. The five-step process will be followed with the CEO.

Step 1: Understand Your Company Profile

To understand their company's profile, they answer the questions provided in the related clause (see clause 5.2 Step 1). They consider the following with respect to UP's profile. UP hosts an online training platform on a company-owned application server in an office they have in a science park. The online platform was developed internally by the UP software engineers. Currently, they have four servers and all employees use company-owned laptops to perform their daily work. UP has one Human Resources (HR) team member who is responsible for all HR related work. They do not have a deep hierarchical structure. A CEO (Chief Executive Officer), a CFO (Chief Financial Officer), three team leaders (Business Development Team, Pre-Sales and Customer Support Team and Development Team), nine team members report to these three team leaders and one HR employee. Their current customers are the companies that work in the same science park with them but UP wants to expand its business. They now have a better understanding of their company in terms of external (i.e. customers, suppliers.) and internal factors (i.e. employees, processes) that can affect its cybersecurity.

Step 2: Perform Security Risk Assessment

They consider the online platform they provide to their customers, the threats they might have for this platform and the vulnerabilities that the software running on their application server might have. They then identify the following risks associated with the threats and vulnerabilities they have thought of:

- They think that an attacker can guess their application server administrator's password and shut their server down. They believe this risk has a low likelihood and a high impact.
- They think that there might be vulnerabilities in the software that could allow DDoS (Distributed Denial of Service) attacks. *The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed [i.23]*. They believe this risk has a medium likelihood and a high impact.

Step 3: Identify Applicable Security Controls

Then, they want to identify which controls they can apply to reduce these risks.

They follow the guidance given at this step and they refer to clause 7 "Four Categories of SMEs in Cybersecurity Context" to identify the category of their company regarding its role in the digital ecosystem. They consider the presented categorization of the Digital SME alliance and identifies their company as "Digitally Based".

Furthermore, they check the recommendations for "Digitally Based" SMEs and understands that their company is in Implementation Group 3 (IG 3). In this recommendation, they are advised to implement all controls present in the Center of Information Security (CIS) Controls. They read the comparative analysis of the standards and frameworks (Table 2) and gets familiar with them. In the comparative analysis, they identify two control categories related to the risks that they have identified. The control category "Access Control" is related to strong passwords and "Secure Development" control category is related to application software security. They decide to investigate these controls deeper using the presented standards and frameworks. They easily find the corresponding controls in the standards and frameworks using the comparative analysis provided in Table 2.

Step 4: Apply Security Controls

As advised in this step, they prepare an implementation plan for the controls that they have selected from the related standards and frameworks based on their risk assessment and prioritization of the risks. An implementation plan example is shown in Table 4.

EXAMPLE: A control implementation plan:

Table 4: Control Implementation Plan Example

Risk #	Control Category	Control	Control Source (Table 2)	Task	Deadline	Responsible
1	Access Control	Use strong passwords	SF4	Ensure that the administrator passwords are strong.	01/08/2020	J. Doe
2	Secure Development	System security testing	SF5	Ensure that security testing is performed.	01/09/2020	D. Smith

In the comparative analysis of the standards and frameworks (Table 2), they notice that there are specific standards and frameworks dedicated to application security (see the last column in Table 2). They decide that it might be good to investigate those; as they want to expand their business and they want to be sure that, their online training platform is cyber-secure. Figure 6 illustrates the asset, vulnerability, threat, and control relationship for the risks of the exemplar SME UP.

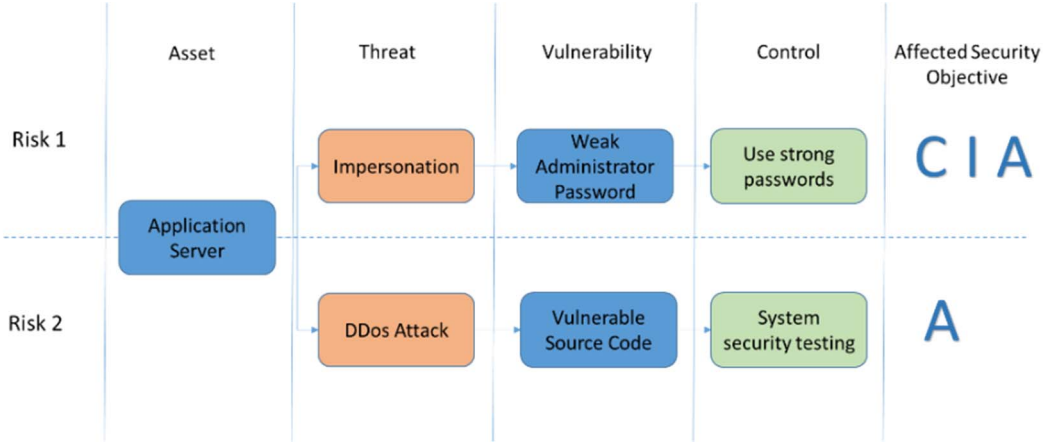


Figure 6: Asset, threat, vulnerability, control relationship for the risks of SME "UP"

Figure 6 shows the asset at risk, vulnerabilities of the asset, the threats that can exploit those vulnerabilities to cause harm and the controls that are chosen to reduce the risks. The conceptual relationships between the assets, vulnerabilities, threats and controls are presented in Figure 3. The CIA triad is presented in Figure 2. Figure 6 presents the affected CIA objectives for the two risks identified for the exemplar SME UP. The cybersecurity risks of UP are certainly more than those two risks presented above. These two risks are highlighted to illustrate how to use the five-step process (Figure 4) presented in the present document to start working on cybersecurity using standards and frameworks.

Step 5: Monitor and Improve

In this step, the CEO checks the status of the task in the implementation plan (Table 4) to take any necessary actions and decides to review the status of the two risks once every six months to see if any other controls are required. SME UP has a plan to migrate its platform to another operating system. The CEO acknowledges that this is a change that might affect the risks. They decide to review the risks before the migration takes place.

Annex A:
SME Standardization and the European Landscape

A.1 Introduction

This annex provides a concise overview of key SME standardization entities and highlights organizations that are at the forefront of standardization for SME cybersecurity throughout Europe.

A.2 EC Rolling Plan for ICT Standardization

With the Communication on ICT Standardization Priorities, the European Commission (EC) proposes to focus standard-setting resources and communities on five priority domains -5G, cloud, cybersecurity, big data and the Internet of Things (IoT) - because they are essential for wider EU competitiveness [i.24]. Every year, the EC releases the Rolling plan on ICT Standardization, which identifies ICT standardization activities in support of EU policies. The rolling plan provides a unique overview of standardization activities in the field of Information and Communication Technologies (ICT) linked to EU legislation and policies, such as healthcare, cloud computing, intelligent transport systems, security, accessibility, Internet of Things, eGovernment, smart grids and many others [i.25]. In the "Cybersecurity/Network and Information Security" section of this plan, EC defines seven actions requested from the Standard Developing Organizations (SDOs). Among these actions, one of them (Action 6) directly addresses SMEs' needs as follows:

SDOs [are] to develop a "guided" version of ISO/IEC 270xx series (information security management systems including specific activity domains) specifically addressed to SMEs, possibly coordinating with ISO/IEC JTC1 SC27 WG1 to extend the existing guidance laid out in ISO/IEC 27003. This guidance should be 100% compatible with ISO/IEC 270xx and help SMEs to practically apply it, including in scarce resource and competence scenarios [i.25].

A.3 Standards Developing Organizations (SDOs)

International, regional or national level Standards Developing Organizations (SDOs) have undertaken several initiatives for helping SMEs in standardization processes. The SME Standardization Toolkit [i.26] is an example of tools provided by CEN and CENELEC to facilitate SME involvement in standardization. This toolkit is mainly aimed for national standardization organization.

Another example to support SMEs in standardization is the SME Toolox of Solutions webpage of CEN/CENELEC [i.27] which provides SMEs with a chance to learn about standardization in a quick and easy way. This webpage is available at https://www.cencenelec.eu/sme/std/Pages/default.aspx .

BSI (The British Standards Institution) has published a guide to standards for small businesses that emphasizes the benefits of standards.

ETSI published a white paper [i.28] on the results of a study to evaluate how to improve the participation of Small and Medium-sized Enterprises (SMEs) in ETSI standardization.

In 2020, ETSI has decided to mandate that proposers of new standards describe their relevance to SMEs. This was published by the Digital SME Alliance as a success story [i.29].

A.4 SME Organizations

This paragraph highlights the Digital SME Alliance and Small Business Standards as organizations that influence cybersecurity for SMEs throughout Europe.

Digital SME Alliance

The European DIGITAL SME Alliance is the largest network of the small and medium sized ICT enterprises in Europe, representing about 20 000 digital SMEs.

SBS: Small Business Standards

Small Business Standards (SBS) is a non-profit organization representing SMEs within the European Standardization System. SBS published a user guide for European SMEs on ISO 26000 guidance on social responsibility [i.30].

Digital SME alliance and SBS have published "SME Guide for the implementation of ISO IEC 27001 on Information Security Management" [i.31].

A.5 Cybersecurity Organizations

This paragraph highlights ENISA and ECSO as organizations that influence cybersecurity efforts throughout Europe.

ENISA: European Union Agency for Network and Information Security

The European Union Agency for Network and Information Security (ENISA) is conducting security surveys and publishing dedicated cyber security guides for SMEs. ENISA has published guidelines for SMEs on the security of personal data processing [i.32] and the cloud security guide for SMEs [i.33]. Another publication of ENISA aims to provide a set of relevant recommendations regarding how to increase the adoption of information security and privacy standards in SMEs [i.34].

ECSO: European Cyber Security Organization

European Cyber Security Organization (ECSO) has a working group (WG 4) to support SMEs that focuses on the following issues [i.35]:

- Support the development of SMEs, start-ups and high growth companies, to help them to create more market transparency and to reach out far beyond their traditional home markets which are usually nationally or regionally limited in order to partner in R&D international projects and access to European market.
- Develop coordinated activities between Regions, Clusters (both business oriented and triple helix) and local bodies (e.g. smart cities) for accelerating the commercialization and scaling up of the interregional innovation projects.

Another working group of ECSO is WG1 "Standardization, certification and supply chain management". This working group addresses the following issues [i.36]:

- Support to the roll-out of the EU ICT security certification framework and its priorities.
- Recommendations on standards to support cybersecurity certification schemes.
- Security assessment guidelines of components, systems and services.
- Impact of security assessment along the supply / value chain in Europe for increased digital autonomy.
- Cooperation with EU and international bodies on standardization and certification.

Finally, ECSO has also published a comprehensive overview of existing cybersecurity standards and certification schemes [i.37].

Annex B:
Starting with Standards and Standardization

B.1 What is a standard and what are the benefits of using standards?

Standards have been a trustworthy resource for individuals, organizations and governments who seek an answer to the question "What is the best way of doing this?" [i.38] and [i.39]. As in every domain, standards on cybersecurity and information security are built on experience and best practices that may help organizations to cope with cyber threats.

The International Organization for Standardization (ISO) states the benefits of standards for small to medium sized enterprises (SMEs) as follows [i.40]:

- Build customer confidence that your products are safe and reliable.
- Meet regulation requirements, at a lower cost.
- Reduce costs across all aspects of your business.
- Gain market access across the world.

Information on the Standards Developing Organizations (SDOs) is given in annex C.

B.2 How to search for the right standards?

The SDOs have search functions on their websites. Searches can be conducted by using any keyword or standard number:

- ISO Standard Search Page: https://www.iso.org/search.html
- CEN Standard Search Page: https://standards.cen.eu/dyn/www/f?p=CENWEB:105::RESET::::
- CENELEC Standards Search Page: https://www.cenelec.eu/dyn/www/f?p=104:104
- ETSI Standard Search Page: https://www.etsi.org/standards-search

The European Commission (EC) Horizon 2020 project StandICT.eu has developed the tool "The European Observatory For ICT Standardisation" [i.41] which monitors the status of ICT standards at the international level, mapping critical areas such as Cybersecurity, 5G, Cloud Computing, IoT, Big Data and Artificial Intelligence. The tool is available at (https://www.standict.eu/euos).

B.3 How to get involved in the standardization processes?

The European Commission (EC) has published guidance for SMEs on how to get involved in standardization processes on its website [i.42]. According to the EC, SMEs are represented by Small Business Standards (SBS) in the standardization process. The EC states that "*SBS directly participates in the standardization process through European Standardization Organizations (CEN, CENELEC, ETSI) and ISO Technical Committees (TCs). With ETSI, SMEs can be involved directly as members and do not have to be represented by SBS.*"

With direct membership, 26 % of ETSI members are SMEs and Micro-Enterprises. ETSI has a dedicated membership page for SMEs at https://www.etsi.org/membership/sme.

Annex C:
Standards Developing Organizations

C.1 International Standardization Bodies

- ISO: International Standardization Organization (www.iso.org):
  - International multisectoral standardization organization active in all fields except the electrotechnical and the telecommunication field.
- IEC: International Electrotechnical Commission (www.iec.ch):
  - International organization active in the electrotechnical area.
- ITU: International Telecommunication Union (www.itu.int):
  - International organization active in the telecommunications area.

C.2 European Standardization Organizations (ESOs)

Three European Standardization Organizations (ESOs), CEN, CENELEC and ETSI have been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at the European level. Only standards developed by the three ESOs (CEN, CENELEC and ETSI) are recognized as European Standards (ENs).

CEN: the European Committee for Standardization (www.cen.eu)

CEN is an association that brings together the National Standardization Bodies of 34 European countries. CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes. CEN supports standardization activities in relation to a wide range of fields and sectors including: air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

CENELEC: the European Committee for Electrotechnical Standardization (www.cenelec.eu/)

CENELEC is responsible for standardization in the electrotechnical engineering field. CENELEC prepares voluntary standards, which help facilitate trade between countries, create new markets, cut compliance costs and support the development of a Single European Market.

ETSI: European Telecommunications Standards Institute (www.etsi.org)

ETSI provides members with an open and inclusive environment to support the development, ratification and testing of globally applicable standards for ICT systems and services across all sectors of industry and society. ETSI is a not-for-profit body with more than 900 member organizations worldwide, drawn from 65 countries and five continents. Members comprise a diversified pool of large and small private companies, research entities, academia, government and public organizations.

A 2020 publication of ENISA provides a comprehensive list of standardization bodies involved in cybersecurity [i.11].

C.3 National Standards Organizations (NSOs)

National Standards Organizations (NSOs) represent countries in the European standardization system. NSOs are responsible for organizing the Public Enquiry in their respective countries as part of the European Standards approval process. They also submit the national position (the 'vote') on the standard. They are also responsible for implementing European standards as national standards. They distribute and sell the implemented European Standard and have to withdraw any conflicting national standards.

CEN [i.43] publishes the list of members on the following webpage:

- https://standards.cen.eu/dyn/www/f?p=CENWEB:5.

CENELEC members are published on the following webpage:

- https://www.cenelec.eu/dyn/www/f?p=web:5.

ETSI publishes its list of NSOs on the following webpage:

- https://portal.etsi.org/TB-SiteMap/NSO/Home.

Annex D:
Maturity Models for Cybersecurity and Information Security

D.1 What is a Maturity Model?

One way of tackling with the challenges of managing and implementing cyber security is using maturity models.

A cybersecurity maturity model provides a structure for organizations to baseline their current cybersecurity capabilities, establishing a foundation for improvement.

Introduced by [i.44], maturity modelling is widely adopted in software engineering and information systems domains following the popularity of CMM for software processes [i.45].

D.2 What are Examples of Maturity Models?

There are several cybersecurity and information security maturity models available. Some of them are presented in Table D.1. In their study, Le and Hoang have identified and analysed 12 different cyber security maturity models [i.46].

Table D.1: Cybersecurity and Information Security Maturity Models

Maturity Model	Organization/Authors	Purpose/Target
Cybersecurity Capability Maturity Model (ES-C2M2) [i.47]	The US Department of Energy (DOE)	Assessment of critical infrastructures
Open Information Security Management Maturity Model (O-ISM3) [i.48]	The Open Group	Any type of organization
National Initiative for Cybersecurity Education - Capability Maturity Model (NICE) [i.49]	The US Department of Homeland Security	Workforce planning for cybersecurity
Information Security Focus Area Maturity model (ISFAM) [i.50]	[i.50]	Any type of organization

D.3 How Can Maturity Models Support Standardization?

Maturity models can help the standardization efforts of the organizations. The capabilities included in the maturity models are usually derived from standards, frameworks, academic literature and best practices from the industry.

Some maturity models are transparent in the way of showing their compatibility with standards and frameworks.

The Open Group's Open Information Security Management Maturity Model (O-ISM3) is an example. Appendix B of this maturity model contains information on Compatibility with other Standards and Frameworks. This enables the users of the maturity model to track the maturity model components to related standards and frameworks.

Annex E: Bibliography

- Yigit Ozkan, B., & Spruit, M.R. (In press): "Cybersecurity Standardisation Essentials for European SMEs", In Fricker, S., Ruiz, J.F., & Tselios, C. (Eds.), SMESEC: Protecting Small and Medium-sized Enterprises digital technology through an innovative cyberSECurity framework. Springer.

- Yigit Ozkan, B., & Spruit, M (2019): "Cybersecurity Standardisation for SMEs: The Stakeholders' Perspectives and a Research Agenda". International Journal of Standardization Research, 17(2), 1-25.

History

Document history		
V1.1.1	May 2021	Publication