EUROPEAN UNION AGENCY
FOR CYBERSECURITY

RISK MANAGEMENT STANDARDS

Analysis of standardisation requirements in support of cybersecurity policy

MARCH 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use mcs@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu

AUTHORS

Ralph Eckmaier, Walter Fumy, Stéfane Mouille, Jean-Pierre Quemard, Nineta Polemi, Rainer Rumpel

Sławomir Górniak – ENISA

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-569-2, DOI 10.2824/001991

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The purpose of this document is to provide a coherent overview of published standards that address aspects of risk management and subsequently describe methodologies and tools that can be used to conform with or implement these standards.

The Regulation (EU) 2019/881 (Cybersecurity Act) states that 'ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services and ICT processes'. (Article 8.5)

This analysis is intended to contribute to the achievement of this goal. It is based on a compiled, comprehensive inventory of standards in the area of cybersecurity risk management and methodologies related to standards. This publication provides guidance to EU Institutions, bodies and agencies on the availability of standards and methodologies relevant to the management of cybersecurity risk and outlines possible gaps in these domains, enabling the relevant EU institutions, bodies and agencies to initiate activities to close these gaps in order to further implement the cybersecurity policies stemming from the legislation.

Furthermore, this publication can also be used by organisations as a library of risk management standards and methodologies for their endeavour to implement risk management within their organisation or in their developments of cybersecurity certification schemes.

Standards are developed and defined through a process of sharing knowledge and building consensus among technical experts nominated by interested parties and other stakeholders. When it comes to developing and establishing standards, a large variety of players exist. Naturally, there is competition between these players but they also cooperate in many instances, in particular when there is a common interest.

Standards are voluntary which means that there is no automatic legal obligation to apply them. However, laws and regulations may refer to standards and even make compliance with them compulsory. This document aims also at providing a brief introduction to the main players when it comes to standards in the area of risk management, introducing the main characteristics of the different document types published by these players, and introducing the inventory of Risk Management Standards presented in the Annex A.

To help this targeted audience in understanding the risk management process and its associated standards, this document is structured in chapters that cover the relevant areas.

Based on the analysis provided in section 5 and making a distinction between risk management standards and risk management methodologies, we propose in section 6 a series of recommendations on the use of risk management standards for various groups of stakeholders – EU decision makers, European SDOs, and ENISA itself.

1. INTRODUCTION

Risk Management is all about identifying and protecting the valuable assets of an organisation. Risk management procedures are fundamental processes to prepare organisations for a future cybersecurity attack, to evaluate products and services for their resistance to potential attacks before placing them on the market, and to prevent supply chain fraud.

1.1 THE PURPOSE OF THIS DOCUMENT

The purpose of this document is to provide a coherent overview of published standards that address aspects of risk management and subsequently list methodologies and tools that can be used to conform with or implement these standards.

This publication will provide guidance to EU institutions, bodies and agencies on the availability of standards and methodologies relevant to risk management and outline possible gaps in this domain, enabling the relevant EU institutions, bodies and agencies to initiate activities to close these gaps.

Furthermore, this publication can also be used by organisations as a library of risk management standards and methodologies for their endeavour to implement risk management within their organisations or develop cybersecurity certification schemes for ICT products, services and processes.

The list of applicable risk management standards and the associated gap analysis provided in this document will be some key inputs in providing content and support in a relevant cybersecurity policy area related to risk management as described in the Cybersecurity Act, Article 8, point 5:

*"ENISA shall facilitate the establishment and take-up of European and international standards for **risk management** and for the security of ICT products, ICT services and ICT processes".*

This document also targets critical sectors as defined in the Annex II of the NIS Directive[1]: Energy, Transport, Banking, Financial market infrastructures, the Health sector, Drinking water supply and distribution, and Digital Infrastructure.

1.2 EU LEGAL REQUIREMENTS

European institutions, bodies and agencies have released several publications – including regulations and directives – concerning the concept of risk management.

These publications are not limited to the classical domain of ICT but also cover transversal or sectorial domains (e.g. maritime, automotive, space, energy, healthcare) with their underlying information security and cybersecurity.

The concept of risk related to the security of ICT infrastructure was initially defined in the first cyber security legislation: The NIS directive - The Network Information Security Directive - Directive 2016/1148.

The directive has placed several legal obligations on ICT security and has also provided a clear definition of how risk is defined in in the context of this directive.

Article 4 (definitions) point (9): '**risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems**.

[1] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

The NIS directive can be considered as the origin of any EU requirement regarding risk management within the ICT domain.

The table here below provides the references on risk management included in the NIS directive.

Table 1: References on risk management in the NIS directive

Article	Point	Text
Recital	Point 4	'Building upon the significant progress within the European Forum of Member States in fostering discussions and exchanges on good policy practices, including the development of principles for European cyber-crisis cooperation, a Cooperation Group, composed of representatives of Member States, the Commission, and the European Union Agency for Network and Information Security ('ENISA'), should be established to support and facilitate strategic cooperation between the Member States regarding the security of network and information systems. For that group to be effective and inclusive, it is essential that all Member States have minimum capabilities and a strategy ensuring a high level of security of network and information systems in their territory. In addition, security and notification requirements should apply to **operators of essential services and to digital service providers to promote a culture of risk management** and ensure that the most serious incidents are reported.'
Recital	Point 44	'Responsibilities in ensuring the security of network and information systems lie, to a great extent, with operators of essential services and digital service providers. **A culture of risk management, involving risk assessment and the implementation of security measures appropriate to the risks faced, should be promoted and developed through appropriate regulatory requirements and voluntary industry practices**. Establishing a trustworthy level playing field is also essential to the effective functioning of the Cooperation Group and the CSIRTs network, to ensure effective cooperation from all Member States.'
Recital	Point 46	**'Risk-management measures include measures to identify any risks of incidents, to prevent, detect and handle incidents and to mitigate their impact**. The security of network and information systems comprises the security of stored, transmitted and processed data.'
Article 7	7,f	'Each Member State shall adopt a national strategy on the security of network and information systems defining the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of network and information systems and covering at least the sectors referred to in Annex II and the services referred to in Annex III. The national strategy on the security of network and information systems shall address, in particular, the following issues:

7, f) **a risk assessment plan to identify risks.**'

Regarding the security of ICT products, ICT services and ICT processes, the crucial EU legal requirements are presented in the Cybersecurity Act Regulation - Regulation (EU) 2019/881 (CSA regulation).

Table 2: References on risk management in the CSA

CSA items	Cybersecurity Act Regulation - Regulation (EU) 2019/881
Risk management as a tool for cybersecurity vulnerability management and remediation	Recital point (11) Modern ICT products and systems often integrate and rely on one or more third-party technologies and components such as software modules, libraries, or application programming interfaces. This reliance, which is referred to as a 'dependency', could pose additional cybersecurity risks as vulnerabilities found in third-party components could also affect the security of the ICT products, ICT services and ICT processes. **In many cases, identifying and documenting such dependencies enables end users of ICT products, ICT services and ICT processes to improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures**.
Importance of European and international risk management standards and methods	Recital (49) Efficient cybersecurity policies should be based on well-developed **risk assessment methods**, in both the public and private sectors. Risk assessment methods are used at different levels, with no common practice regarding how to apply them efficiently. Promoting and developing best practices for risk assessment and for interoperable risk management solutions in public-sector and private-sector organisations will increase the level of cybersecurity in the Union. **To that end, ENISA should support cooperation between stakeholders at Union level and facilitate their efforts relating to the establishment and take-up of European and international standards for risk management and for the measurable security of electronic products, systems, networks and services which, together with software, comprise the network and information systems.**
Creating the link between the ICT risk management from the NIS directive and the CSA regulation	**Article 5: Development and implementation of Union policy and law** ENISA shall contribute to the development and implementation of Union policy and law, by: (2) assisting Member States to implement the Union policy and law regarding cybersecurity consistently, **in particular in relation to Directive (EU) 2016/1148, including by means of issuing opinions, guidelines, providing advice and best practices on topics such as risk management,** incident reporting and information sharing, as well as by facilitating the exchange of best practices between competent authorities in that regard.
Promoting and facilitate the establishment of European and international standards for ICT risk management	Article 8: Market, cybersecurity certification, and standardisation **Point 5**. **ENISA shall facilitate the establishment and take-up of European and international standards for risk management and for the security of ICT products, ICT services and ICT processes.**

The next table provides a non-exhaustive list of existing EU legislative acts (transversal or sectorial) where the concept of risk or risk management for information security or cybersecurity aspects is included:

Table 3: non-exhaustive list of existing EU legislation texts containing risk management

CSA	**Cybersecurity Act Regulation- Regulation (EU) 2019/881**
NIS	Network Information Security Directive - **Directive 2016/1148**
eIDAS	Electronic Identification and Trust Services for Electronic Transactions -

	Regulation (EU) No 910/2014
GDPR	General Data Protection Regulation - **Regulation (EU) 2016/679**
PSD2	Directive on payment services in the internal market – **Directive (EU) 2015/2366**
AML	Anti-Money Laundering Directive - **Directive (EU) 2015/849**
RED	Radio Equipment Directive- **Directive 2014/53/EU (RED)**

In Annex B an example of how ICT risk and risk management are addressed in the existing eIDAS regulation (Electronic Identification and Trust Services for Electronic Transactions – Regulation (EU) No 910/2014) is presented.

At the time of publishing this document, the European Commission is preparing new or amended legislation containing the concept of risk management (see table below).

Table 4: non-exhaustive list of proposed EU legislative acts containing risk management

NIS V2	Directive on security of network and information systems V2
eIDAS V2	EU regulation on electronic identification and trust services for electronic transactions in the European Single Market
Artificial Intelligence Act	Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts COM/2021/206 final
ePrivacy regulation	Proposal for a Regulation of the European Parliament and of the Council concerning respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final - 2017/03 (COD)
Digital Service Act	Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final

1.3 ENISA WORK ON RISK MANAGEMENT

Since its creation ENISA has worked on the risk management issue and has produced several documents on this topic.

Table 5: Non-exhaustive list of relevant ENISA publications

Editor	**Publication name**
ENISA	Methodology for a Sectoral Cybersecurity Assessment
ENISA	Threat Landscape for Supply Chain Attacks
ENISA	Guidelines - Cyber Risk Management for Ports

ENISA	National-level Risk Assessments: An Analysis Report
ENISA	Consumerisation of IT: Final report on Risk Mitigation Strategies and Good Practices
ENISA	Inventory of Risk Management / Risk Assessment Methods and Tools
ENISA	Guidelines for trust service providers - Part 2: Risk assessment
ENISA	Cloud Computing Risk Assessment
ENISA	Methodology for sectoral cybersecurity assessments

Apart from the relevant work conducted by ENISA in this area, the European Commission has funded a number of research projects related to Risk Management. The references can be found at https://cordis.europa.eu/ .

2. SCOPE AND DEFINITIONS

2.1 SCOPE OF THE ANALYSIS

The Regulation (EU) 2019/881 (Cybersecurity Act) states that '**ENISA shall facilitate the establishment and take-up of European and international standards for risk management** and for the security of ICT products, ICT services and ICT processes'. (Article 8 no. 5)

This analysis is intended to contribute to the achievement of this goal. It is based on a compiled and comprehensive inventory of standards (Annex A) in the area of cybersecurity risk management and methodologies related to standards. Special attention is given to the analysis of gaps and overlaps of the available standards.

The analysis aims to identify practical ways to apply these standards by different stakeholders, compiling guidelines and good practices.

2.2 NEEDS OF STAKEHOLDERS IN RELATION TO RISK MANAGEMENT

More and more organisations understand that cybersecurity and information security risks have to be managed because corresponding threats can have substantial consequences to the organisation or even threaten its existence.

As stated in the introduction, this publication shall provide guidance to EU institutions, bodies and agencies, as well as to various organisations, to be used as a library of risk management standards and methodologies for their endeavour to implement risk management processes.

Many of these stakeholders are looking for advice on which standards or methodologies are suitable for their organisation. Small companies are often overwhelmed by what is offered in the market and find choosing suitable methods difficult. This paper also presents methodologies for small companies (e.g. OCTAVE-S). When implemented, risk management approaches are influenced by the sector in which the organisation does its business. There are sector-specific risk management standards and methodologies that take into account the related specifics.

2.3 DEFINITIONS

2.3.1 Risk management

Risk

There are two slightly different definitions within documents published by the ISO and the IEC that are relevant for risk management. These are listed for comparison in the following table.

Table 6: Comparison of risk definitions in ISO standards and directives

Effect of uncertainty on objectives	Effect on uncertainty
[SOURCE: ISO 31000:2018] [SOURCE: ISO/IEC 27000:2018]	[SOURCE: ISO Directives, Part 1, Annex SL, Appendix 2]
Note 1: an effect is a deviation from the expected. Certain organisations consider positive deviations in addition to negative	Note 1 to entry: an effect is a deviation from the expected — positive or negative. Note 2 to entry: uncertainty is the state, even

deviations in the risk context. Note 2: risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood. Note 3: uncertainty is the state, even partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood. Note 4: objectives are not only but often are related to business, organisation or projects. Another level of objectives is presented in section 3.1.	partial, of deficiency of information related to understanding or knowledge of an event, its consequence, or likelihood. Note 3 to entry: risk is often characterised by reference to potential events (as defined in ISO Guide 73) and consequences (as defined in ISO Guide 73) or a combination of these. Note 4 to entry: risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (as defined in ISO Guide 73) of occurrence.

As stated in the comparison table above, there are slightly diverging definitions of risk within the ISO domain. These definitions diverge depending on whether a risk is connected to a defined objective (ISO 31000) or not. In the context of a management system standard, such as ISO/IEC 27001, risks can arise regardless of whether objectives have been set in advance.

ISO/IEC 27000:2018 contains the definition of ISO 31000:2018 because the ISO 31000 definition is referenced in ISO/IEC 27005.

For ISO/IEC 27001, the definition of Annex SL is relevant, as ISO/IEC 27001 has to follow the text of the ISO Directives.

For example, the sector-specific standard ISO/SAE 21434:2021 follows the definition on the right-hand side of the table, that risk is the 'effect on uncertainty on road vehicle cybersecurity'.

In Directive (EU) 2016/1148 ('NIS Directive') there is a different definition of risk. Article 4 states that risk is 'any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems'. Compared with the definitions given by ISO standards and directives the focus here is on the threat component in relation to the source of risk not to the effect. Cf. ISO/IEC 27005 DIS (2021) Clause 8,2,3.

Risk management

Coordinated activities to direct and control an organisation with regard to risk.

[SOURCE: ISO 31000:2018]

Note: the essential elements of risk management are risk assessment and risk treatment or mitigation.

Risk assessment

Overall process of risk identification, risk analysis and risk evaluation.

[SOURCE: ISO Guide 73:2009]

Risk treatment

Process to modify risk.

[SOURCE: ISO Guide 73:2009]

Note: risk treatment can be carried out using different options, e.g. avoiding the risk or changing the likelihood (of events or consequences).

2.3.2 Standards and methodologies

What is a **standard**?

A standard is a document generally established by consensus and approved by a recognised body that provides rules or guidance on the design, use or performance of materials, products, technologies, processes, services, systems or persons.

Standards can be developed by national, regional and international standards developing organisations[2] (e.g. ISO, IEC, CEN, ETSI, DIN).They can also be developed by consortia of businesses to address a specific marketplace need or by government departments to support regulations. Not every standard is called a 'standard'. For example, another common name used is Technical Specification. In this case, as a rule, a qualified majority may also be sufficient for the adoption of the document.

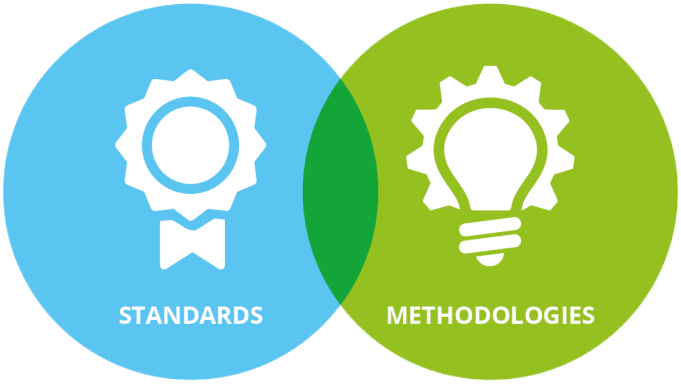
A more extensive description of standard developing organisations and their deliverables is provided in chapter number 4.1. of this document (section 4.1.1.)

What is a **methodology**?

A methodology is a set of principles and methods (at least one) adhering to good practices used to perform a particular activity. It's a coherent and logical scheme that guides the choices users of the methodology make.

What is the **relation** between standards and methodologies?

Some methodologies are (published as) standards and some standards include methodologies.



Option 1: Methodology is used to achieve conformance to a standard (with reference in part or in whole to a certain standard and its requirements).

Option 2: Methodology is given as a standard and can be used to achieve conformance to a standard and its requirements.

Option 3: Methodology is a set of good practices but not related to any standard and not used to achieve conformance.

[2] Abbreviation: SDO

A methodology clarifies how certain issues should be handled. The methodology is often defined through test-specifications related to a standard. If a methodology is given as a standard the same is true. Moreover there are also many standards which focus on what to do and not how to do (mainly requirements standards).

Table 7: Examples of methodologies, which are published as standards

ISO 13053-1:2011	Quantitative methods in process improvement — Six Sigma — Part 1: DMAIC methodology
ISO/IEC 18045:2008	Information technology — Security techniques — Methodology for IT security evaluation
ETSI TS 102 165-1:2017	CYBER — Methods and protocols — Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)

2.3.3 Risk management vocabulary

The vocabulary of risk management is often different between standards and methodologies. It can be observed that the definitions of terms used in well-known ISO standards and guides (Table 8) are quite similar while there are clear differences in other standards (e.g. in Table 9). ISO definitions are compact while others are more extensive. The definition of risk acceptance is missing in NIST and BSI Germany.

Table 8: Examples of risk management terms in ISO standards and guides

Term	ISO 31000 (2018)	ISO/IEC DIS 27005 (2021)	ISO Guide 73 (2009)
risk management	coordinated activities to direct and control an organisation with regard to risk	---	coordinated activities to direct and control an organisation with regard to risk
risk assessment	overall process of risk identification, risk analysis and risk evaluation	overall process of risk identification, risk analysis and risk evaluation	overall process of risk identification, risk analysis and risk evaluation
risk acceptance	retaining the risk by informed decision	informed decision to take a particular risk	informed decision to take a particular risk

Table 9: Examples of risk management terms in some other standards

Term	NIST SP 800-39 (2011)	BSI Germany Standard 200-3
risk management	process that requires organisations to: (i) frame risk; (ii) assess risk; (iii) respond to risk; and (iv) monitor risk.	consists of the following steps: risk assessment; risk evaluation; determination of safeguards for treating risks; comparison between the costs of every safeguard and the damage to be expected and decision in favour of or against the implementation of the safeguard; examination of the residual risks: definition of handling options; comparison with opportunities; monitoring of the risks and adjustment of the safeguards or handling options during live operation.

risk assessment	The purpose is to identify: (i) threats to organisations or threats directed through organisations against other organisations or the nation; (ii) vulnerabilities internal and external to organisations; (iii) the harm to organisations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur.	is the determination of the frequency of occurrence of the threat and extent of damage.
risk acceptance	---	---

2.4 ROLE OF RISK MANAGEMENT STANDARDS IN CERTIFICATION SCHEMES

2.4.1 Introduction

There are many relations between risk management processes and standards.

Risk management consists of the following steps:

1. Identification of threats

In this phase the various threats or threat models are identified according to different methods. For example, the assets to be protected are listed according to the risk management policy and the relevant potential threats are listed. Threat identification can also be done according to other methods such as the identification of vulnerabilities or threat models. Standards can provide a checklist to help with identifying different assets, threats or vulnerabilities consistent with particular regulations (for example NIS or GDPR).

2. Evaluation of threats

The different threats are evaluated according to different sources. For example, cyber threat intelligence (CTI) can be used or standards on the ontology and terminology of threats. Standards can provide guidance on threat selection according to the security profile selected.

3. Evaluation of risk

The risk evaluation process is key to defining how to use the scale of threats, impacts, likelihood and occurrence parameters in order to prioritise different threats. Here, standards are of strong interest.

4. Mitigation of risk

Risk mitigation is the answer you will put in place in order to handle the risks identified. Risk management standards like ISO/IEC 27005 or EN 303 645 are helpful examples.

5. Evaluation and assessment of risk controls

In this last step we will evaluate implemented security controls, check their efficiency and assess the mitigation of security risk.

2.4.2 ICT Products certification

> An **ICT product** *means an element or a group of elements of a network or information system.*
>
> Definition from EU Cybersecurity Act

A well-known framework for evaluating and certifying ICT products, which also became an international standard is *Common Criteria for Information Technology Security Evaluation*[3]. EN ISO/IEC 15408 establishes the concepts, principles and techniques for IT security evaluation.

The standard consists of three parts: the EN ISO/IEC 15408-1:2020[4] that introduces the general concepts and model, the EN ISO/IEC 15408-2:2020[1] that includes the security functional components and the EN ISO/IEC 15408-3:2020[1] that describes the security assurance components.

ISO/IEC 18045:2020[1] is a companion standard for the ISO/IEC 15408 family and provides a methodology to help an IT security evaluator to conduct a CC evaluation by defining the minimal actions to be performed.

The IT Security of ICT products is concerned with the protection of assets. Assets according to EN ISO/IEC 15408-1:2020 include the integrity of the contents of a database, the availability of an electronic workflow, the authenticity of requests received by a webserver. The information of many assets is stored, processed and transmitted by ICT products to meet the requirements specified by the owner of the information.

Due to the CC security concept the information owner who wishes to minimise the risk to an asset is exposed by imposing countermeasures. The selection of countermeasures depends on the threats identified for the asset, consideration of the likelihood of the threat being realised and the impact on the asset when a threat is realised. CC distinguishes between IT countermeasures and non-IT countermeasures.

An example of a sector-specific standard for risk management of assets is EN ISO 14971:2019 Medical devices — Application of risk management to medical devices.

To become a CC evaluation body it is necessary to conform to the requirements written in EN ISO/IEC 17025:2017. ISO/IEC 17000-series (17000:2020, 17020:2012, 17021:2015, 17024:2012, 17025:2017 and 17067:2013) is an international set of standards that mainly provides from general concepts and principles for Conformity Assessment (CA) to guidelines, good practices and requirements for bodies serving as certification authorities.

2.4.3 Management system certification

> An **ICT service** *means a service consisting fully or mainly in the transmission, storing, retrieving or processing of information by means of network and information systems.*
> An **ICT process** *means a set of activities performed to design, develop, deliver or maintain an ICT product or ICT service.*
>
> Definition from EU Cybersecurity Act

There are several international standards defining requirements for the certification of management systems. The list includes:

- ISO 28000:2009: Specification for security management systems for the supply chain;

[3] Common Criteria is abbreviated to CC.
[4] A new edition is available as DIS.

- ISO 45001:2018 Occupational health and safety management systems; requirements with guidance for use;
- EN ISO 50001:2018 which specifies requirements for establishing, implementing, maintaining and improving an energy management system (EnMS);
- ISO/IEC 20000-1:2018 Information technology — Service management — Part 1: Service management system requirements;
- EN ISO/IEC 27001: 2017 Information technology - Security techniques - Information security management systems[5] – Requirements.

If an organisation intends to certify an ICT service or an ICT process or a group of these (called 'entity' as of now), then it is suitable to define this entity as the scope of its management system. On this basis, ICT services or ICT processes can be certified by assessing their conformity to the requirements specified in ISO/IEC 20000 or EN ISO/IEC 27001.

When an organisation intends to achieve conformance with the requirements of a management system standard such as EN ISO/IEC 27001:2017, the requirements addressing risk management can be found in these clauses:

- 6.1 Actions to address risks and opportunities
- 8.2 Information security risk assessment
- 8.3 Information security risk mitigation.

Whereas sub-clause 6.1.1 addresses high-level risks such as management system risks and strategic risks, the sub-clauses 6.1.2 and 6.1.3 specify requirements regarding the management of risk for the security of operational information.

ISO/IEC 27005 (Information security risk management) offers closely aligned support for implementing the requirements for risk management in entities within the scope of the ISMS. Furthermore, among others, the following standards are helpful:

- ISO 31000 – Risk management guidelines (general perspective)
- BSI 7799-3 – Guidelines for information security risk management
- NIST SP 800-39 – Managing Information Security Risk
- BSI Germany Standard 200-3 - Risk analysis based on IT-Grundschutz

Examples of sector-specific standards for risk management in the context of a management system are:

- BS 31111:2018 Cyber risk and resilience: Guidance for the governing body and executive management services (also useful for ICT product certification);
- ISO/FDIS 23314-2 Ships and marine technology — Ballast water management systems (BWMS) — Part 2: Risk assessment and risk reduction of BWMS using electrolytic methods;
- ASTM F3449-2 Standard Guide for Inclusion of Cyber Risks into Maritime Safety Management Systems and services in Accordance with IMO Resolution MSC.428(98)-Cyber Risks and Challenges.

Conformance to ISO/IEC 27001 can be confirmed by certification bodies, which are accredited in conformity with the families of standards ISO/IEC 17021 and ISO/IEC 27006.

[5] abbreviation: ISMS

3. BASELINE ANALYSIS

3.1 OBJECTIVES OF RISK MANAGEMENT

The main objective of risk management within an organisation is to determine possible uncertainties or threats, to protect against resulting consequences and to permit the achievement of business objectives.

The objectives of risk management can be derived from the overall objectives of the organisation, its business and legal obligations.

These objectives must be clearly defined at the beginning of the risk management process. These objectives must also be measurable in order to be able to verify their achievements. The use of KPIs (key performance indicators) is recommended. The objectives must be related to the assets of the entity that are to be protected against risks and their consequences.

These objectives are determined during the establishment of the context of a risk management process (see Clause 3.3. Risk management process).

3.2 RISK MANAGEMENT PROCESSES

The risk management process is the individual way in which an organisation addresses the concept of risk and the relevant types of risk within itself. The risk management process is a fundamental part of any organisation and has to be integrated into all relevant (business) processes and activities, and if necessary – based on the type and nature of the business of the organisation – on several layers.

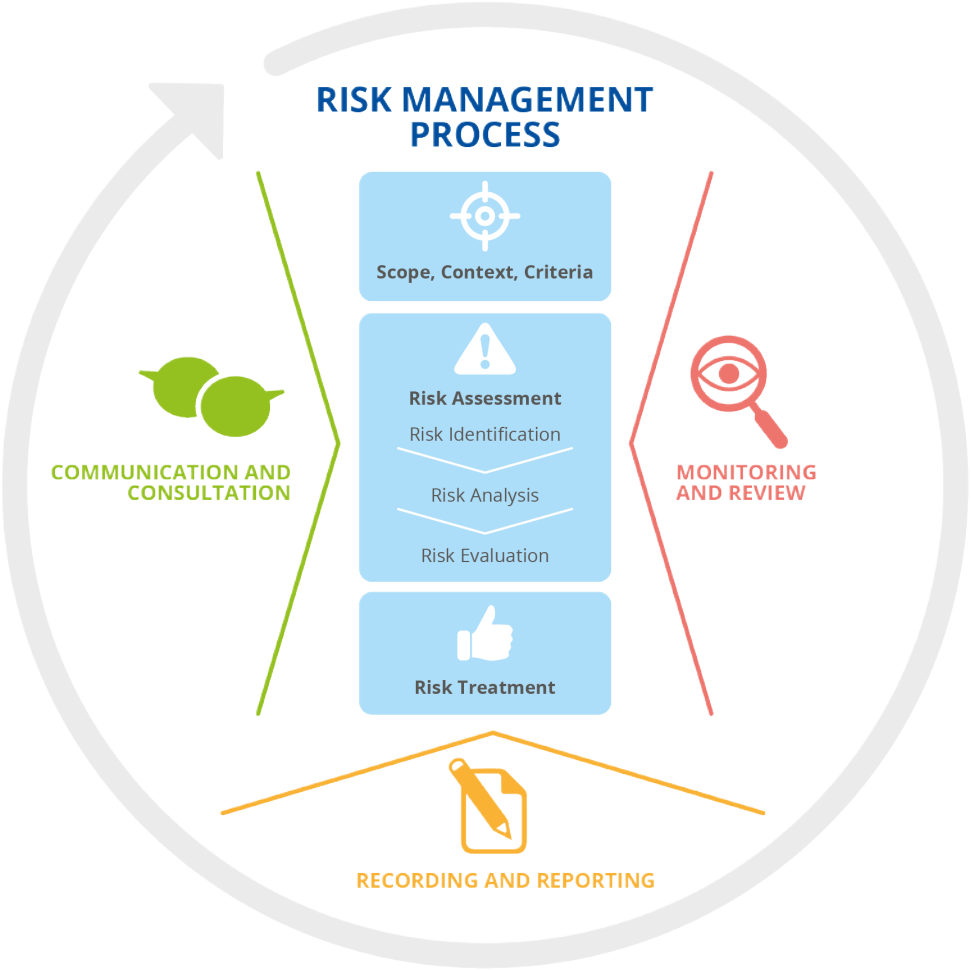
If an organisation wants to achieve conformance with a management system standard (type A) based on the ISO Directives, Annex SL, Appendix 2, the risk management process is one of the fundamental and essential processes within the organisation within the scope of the management system. Nevertheless, ISO 31000:2018 does not give guidance on a risk management system but describes a risk management framework. EN ISO/IEC 27001:2018 is a management system standard based on the Harmonised Framework and requires a risk management process in clauses 6.1, 8.2 and 8.3.

Risk management may address individual types of risks, such as enterprise risk, market risk, credit risk, operational risk, project risk, development risk, supply chain risk, infrastructure risk, component risks or several of the risk types listed or all of them. This list is not exhaustive and depending on the type of business an organisation has, additional types of risks may exist and be of relevance.

In the context of this document which addresses cybersecurity and information security, these types of risks have to be assessed in conjunction with the three properties of information security – confidentiality, integrity and availability. For example, what consequences may arise for market risk from a loss of integrity, or what consequences may arise for supply chain risk from a loss of confidentiality, and so on?.

In the context of this document, the elements of the risk management process contained in ISO 31000:2018 will be applied to describe a possible implementation of a risk management process within an organisation. Independent of the organisation's actual implementation of its risk management process, all activities outlined in ISO 31000:2018 will be more or less present, independently of whether such a risk management process is integrated into an organisation

seeking conformance with EN ISO/IEC 27001:2018 or any other ISO management system standard.



Scope, Context, Criteria

When establishing risk management within an organisation, the fundamental decisions regarding the risk management process itself are made during the determination of the scope, the context and the criteria.

Based on the scope of the risk management, different sub-processes using several risk assessment methodologies may be applied within an organisation.

The scope may be derived from:

- the relevant internal and external interested parties;
- its level of application (strategic, operational, programme, project, supply-chain, product development, software development);
- its inclusion into a formal management system;
- its relationships to other organisations, entities, activities, projects, processes;
- its objectives;
- the available resources (personnel, software tools, etc.)[6].

[6]This list is not exhaustive.

Risk management addressing information security or cybersecurity may also involve different application domains:

- critical infrastructure (health, electricity, communication etc.);
- sensitive data;
- supply chain.

When it comes to the context, this may depend on:

- the interested parties (external and internal),
- the objectives and activities of the organisation,
- the purpose of the risk management,
- the integration into an existing risk management framework or management system.

During the determination of the criteria in this early stage of establishing risk management, the organisation, based on the previous results of determining the scope and the context, also determines:

- the type of risk it is managing,
- the risk assessment methodology to apply,
- the criteria for evaluation the risks,
- the criteria for accepting risk.

Thereafter, the risk criteria as determined have significant consequences on the subsequent activities of a risk management process, such as risk assessment and risk mitigation.

Risk assessment

Risk assessment is most commonly composed of threats identification, threats evaluation, risk analysis and risk evaluation (see Figure 1).

Depending on the decisions taken during the *scope, context* and *criteria* activities, different methodologies may be implemented for different types of risks and for different layers.

Threats identification is the activity of finding and describing threats systematically and should consider the following factors:

- sources of risk,
- causes and events,
- threats and vulnerabilities,
- emerging risks and threats,
- nature and value of assets,
- consequences and impact on processes and assets[7].

During risk analysis, the factors listed above are used to comprehend the nature and the level of a threat or risk based on factors such as:

- the likelihood of an event, threat or risk;
- the magnitude of consequences triggered by an event, threat or risk;
- the complexity including possible links, dependencies and cascading effects;

[7]This list is not exhaustive.

- the effectiveness of existing controls;
- time-related factors such as volatility or the period under consideration.

The results of the risk analysis provide the input to the risk evaluation in which the results from the risk analysis are compared to the previously established risk criteria including the criteria for the acceptance of risk. These results may be calculated based on criteria for consequence and likelihood, or by using other means such a heat maps or tables.

Risk treatment

Risk treatment (as defined in, among others, ISO 31000) is the activity of selecting an adequate option for treating risks that are above a previously defined acceptable risk level.

These options are:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing the risk in order to pursue an opportunity;
- mitigating the source of the risk;
- changing the likelihood;
- changing the impacts and consequences;
- sharing the risk (e.g. through contracts, buying insurance);
- retaining the risk through an informed decision.[8]

The selected risk treatment option must be approved by the risk owner and documented. Based on this decision, a risk treatment plan shall be formulated and approved by the risk owner, and implemented according to the project plan included in the risk treatment plan.

A risk treatment plan and the newly introduced controls may result in new risks or threats that need to be addressed separately.

The other elements of Figure 1 (Communication and Consultation, Recording and Reporting, Monitoring and Review) are, in the context of this document, considered not to be part of the risk management process but rather established parts of a management system based on an ISO management system standard and are therefore not covered in this document.

Note: risk treatment that deals with negative consequences is sometimes referred to as risk mitigation'.

3.3 USE OF STANDARDS IN RISK MANAGEMENT

When integrating the concept of risk management into its organisation, an entity is looking for appropriate approaches that are adequate for their business and the scope and the objective of their risk management efforts.

Organisations may decide that they need an overall enterprise risk management to address all types of risks (such as operational risk, market risks, supply chain risks, project risks or strategic risks) or just a specific type of risk (see examples of risks previously stated).

For these different scopes and objects, and specific to the organisations' main business activities, different risk assessment and treatment models may be used.

[8]This list is from ISO 31000: 2018, Clause 6.5.2

Thus, organisations may wish to learn from other organisations in their field of business and try to establish approaches to best practices that seem to fit them and others in their discipline or field of activities.

Based on this goal, it is common to find that risk assessment or risk treatment models for specific sectors or businesses are developed by sector associations or interest groups. Many times, these sector or discipline-specific models evolve into international standards by forwarding their results to the technical committee of an international or European standardisation organisation.

Being considered as a standard by an international community of experts and thereby gaining wider attention and improvement, enables additional organisations to find adequate solutions to fulfil their needs regarding the assessment and treatment of risks.

Such standards can provide generic guidance on terminology, principles, process models and treatment options (e.g. ISO 31000) as well as detailed descriptions of risk assessment models (e.g. ISO/IEC 31010, ISO/IEC 27005).

Applying these different standards at different levels of an organisation can enhance the reproducibility of results, enable the comparison of different organisations and support the evaluation of the processes involved and their results within an organisation. Applying the same standard within a discipline or sector also provides the ability to benchmark one organisation against another or against an average for a sector or an entire discipline.

Standards, in principle, also enable organisations to estimate and compare the suitability, the effectiveness, the efficiency and the coverage of individual models and methods for a specific sector or discipline of a business and thereby support organisations in choosing an adequate standard for integration into their organisation.

Not only standards that especially address and describe risk assessment and risk treatment methods are important for the integration of the concept of risk management into an organisation. Widely accepted management system standards, such as ISO 9001 (Quality management system), ISO 14001 (Environmental management system) and ISO/IEC 27001 (Information security management system), have the concept of risk awareness integrated in their requirements and thus mandate the concept of risk management should an organisation claim conformance to these management system standards.

4. STANDARDS AND METHODOLOGIES

4.1 RISK ASSESSMENT STANDARDS

Standards are developed and defined through a process of sharing knowledge and building consensus among technical experts nominated by interested parties and other stakeholders. When it comes to developing and establishing standards, there is a large variety of players. Naturally, there is competition between these players but they also cooperate in many instances, in particular when there is a common interest.

Standards are voluntary which means that there is no automatic legal obligation to apply them. However, laws and regulations may refer to standards and even make compliance with them compulsory.

The following sections:

- provide a brief introduction to the main players when it comes to standards in the area of risk management;
- introduce the main characteristics of the different document types published by these players;
- introduce the inventory of risk management standards as presented in Annex A of this document.

4.1.1 European SDOs (ESOs) and European Standards

European Standards (ENs) are documents that have been ratified by one of the three European Standardisation Organisations (ESOs), CEN, CENELEC or ETSI, and are recognised as competent in the area of voluntary technical standardisation in accordance with EU Regulation 1025/2012.

- CEN, the European Committee for Standardization, reflects the economic and social interests of 34 CEN Member countries channelled through their national standardisation organisations and provides a platform for the development of European standards and other technical documents in relation to a wide range of fields and sectors including air and space, consumer products, defence and security, energy, health and safety, ICT, machinery, services, smart living, and transport.
- CENELEC is the European Committee for Electrotechnical Standardisation and is responsible for standardisation in the electro-technical engineering field.
- ETSI addresses the ICT domain with particular focus on the communications aspects for connected devices and the networks that connect them.

A European Standard (EN) 'carries with it the obligation to be implemented at national level by being given the status of a national standard and by the withdrawal of any conflicting national standard'. Therefore, a European Standard (EN) automatically becomes a national standard in each of the 34 CEN-CENELEC member countries.

ESO deliverables also include the following.

- CEN/CENELEC Workshop Agreement (CWA): a CWA is a CEN-CENELEC agreement, developed by a workshop, which reflects the agreement of identified

individuals and organisations responsible for its contents. A CWA does not have the status of a European Standard and CEN-CENELEC national members are not obliged to withdraw national standards in conflict with a CWA.

- ETSI Standard (ETSI ES) and ETSI Guide (ETSI EG) are ETSI deliverables adopted after weighted voting by ETSI members.
- An ETSI Technical Specification (ETSI TS) and an ETSI Technical Report (ETSI TR) are ETSI deliverables adopted by the responsible Technical Body.

Within the three European SDOs, CEN-CENELEC Joint Technical Committee 13 'Cybersecurity and Data Protection' (CEN-CLC JTC 13) has published several standards in the area of risk management (see Annex A), most of them having been adopted from SC 27 publications. ENISA maintains a strong liaison with JTC 13 and maintains regular contact.

4.1.2 International SDOs and Standards

An International Standard (IS) is a document that has been developed through the consensus of experts from many countries and has been approved and published by one of the globally recognised international SDOs:

ISO: the International Organization for Standardization (ISO) is an independent international organisation, with a membership of 165 national standards bodies, that develops voluntary, consensus-based international standards. Within ISO, TC 292 provides a family of standards in the area of risk management (e.g. ISO 31000) while most cybersecurity related activities take place within subcommittee SC 27 of Joint (with IEC) Technical Committee 1 (ISO/IEC JTC1/SC27). ENISA liaises with SC 27 and maintains regular contact.

- IEC: the International Electrotechnical Commission (IEC) develops international standards for all electrical, electronic and related technologies.
- ITU (the International Telecommunication Union): has a Study Group SG17 – Security where areas of cybersecurity are discussed. Currently this SDO is relatively less advanced in the field of cybersecurity and thus can be considered as a secondary priority.

Deliverables also include:

- Technical Specifications: a Technical Specification (TS) developed by an international SDO addresses work still under technical development, or where it is believed that it will eventually be transformed and republished as an International Standard.
- Technical Reports: a Technical Report (TR) is more informal than an IS or TS; it may, for example, include data from an informative report or information on the perceived 'state of the art'.

4.1.3 National standardisation bodies and specialised agencies

National standardisation bodies and specialised agencies in the EU are also directly represented in the ESOs and, in many instances, their national publications eventually become European Norms or International Standards. However, the inventory established in Annex A of this document refers to several risk management standards available solely from national standardisation bodies and specialised agencies. Examples of such bodies include the following.

- BSI: the Federal Office for Information Security (BSI) in Germany is a national cyber security authority, promoting IT security in Germany and also developing cybersecurity standards and guidelines. BSI standards and technical reports are available at no cost from www.bsi.bund.de.

- NIST: the National Institute of Standards and Technology (NIST) is part of the US Department of Commerce. Its Information Technology Laboratory (ITL) is one of six research laboratories within NIST. ITL has seven divisions including the Applied Cybersecurity Division (ACD) and the Computer Security Division (CSD), both developing cybersecurity standards and guidelines. CSD publications include the Risk Management Framework NIST SP 800-37. NIST standards and guidelines are available at no cost from www.nist.gov.
- ANSSI (Agence Nationale de la Sécurité des Systèmes d'information), the French National Cybersecurity Agency has been involved in risk management methodology and processes. In particular ANSSI has been promoting the EBIOS risk manager methodology.

4.1.4 Industrial bodies

Industrial bodies and fora are not considered formally as SDOs; however, they offer de-facto standards in certain areas including risk management. Where applicable, the output of industrial bodies is included in the inventory established in Annex A of this document.

As an example, OASIS began as a consortium of vendors and users and today is a large non-profit standards organisation advancing projects for, among others, cybersecurity, blockchain, IoT, emergency management, and cloud computing. OASIS often submits specifications produced by its TCs to other standards bodies (e.g. ISO/IEC JTC 1, ITU-T, ETSI) for additional ratification.

In particular, the OASIS TC Collaborative Automated Course of Action Operations (CACAO) for Cyber Security aims to create standards that implement the course of action playbook model for cybersecurity operations.

A second example is the Institute of Electrical and Electronic Engineers Standards Association (IEEE SA), an entity within IEEE that develops global standards in a broad range of areas. As with OASIS, some IEEE specifications are submitted to 'official' SDOs for additional ratification, such as IEEE/ISO/IEC 16085:2020 - Systems and software engineering - Life cycle processes - Risk management.

Important work in the area of risk management is also undertaken by GSMA,

4.1.5 The Risk Management Standards Inventory

Annex A of this document provides an inventory of almost fifty identified standards which relate to risk management. The documents are characterised by:

- document source, e.g. national standard, European standard, international standard;
- document type, e.g. standard, technical specification, technical report;
- document scope, e.g. risk management vocabulary and guides, risk management requirements, risk management evaluation methodology.

The inventory also provides information about applicable technical domains, document history, and relevancy to EU legislation.

The following standards in the inventory are considered most relevant for risk management in the context of information and cybersecurity and are thus labelled 'Risk management' in column E (document scope) of the table.

- ISO/IEC 27005 – Information security risk management
  This document was developed using ISO/IEC JTC 1/SC 27 and provides general

guidelines for information security risk management in an organisation without promoting any specific risk management method.

- ISO 31000 – Risk management guidelines
  This document was developed by ISO TC 292 and provides principles, a framework and a process for managing risk from a general perspective. The Australian and New Zealand version AS/NZS ISO 31000:2009 is identical to and reproduced from ISO 31000:2009.
- BSI 7799-3 – Guidelines for information security risk management.
- NIST SP 800-39 – Managing Information Security Risk
  This document developed by NIST provides guidance for an integrated, organisation-wide programme for managing information security risk to organisational operations.
- BSI Germany Standard 200-3 – Risk analysis based on IT-Grundschutz
  This methodology developed by the German Federal Office for Information Security demonstrates how the threats listed in the IT-Grundschutz Catalogues can be used to carry out a simplified analysis of risks for information processing.

4.1.6 Risk management methodologies and tools

The main goal of risk management is (in general) to protect ICT products (software, hardware, systems, components, services) and business assets, and minimise costs in cases of failures. Thus it represents a core duty for successful business or IT management. Hence, risk management describes a key activity for security within organisations and it is essentially based on the experience and knowledge of methods of best practice and the tools that can be used.

These methods consist of an estimation of the risk situation based on the business process models and the infrastructure within the organisation. In this context, these models support the identification of potential risks and the development of appropriate protective measures. The major focus lies on companies and the identification, analysis and evaluation of threats to their respective corporate values.

The outcome of a risk analysis is in most cases a list of risks or threats to a system, together with the corresponding probabilities. International standards in the field of risk management are used to support the identification of these risks or threats as well as to assess their respective probabilities. These standards (see Annex A) range from general considerations and guidelines for risk management processes to specific guidelines for the IT sector (all the way to highly specific frameworks as, for example, in the maritime sector. Most of these standards specify framework conditions for the process of risk management but rarely go into detail on specific methods for the analysis or assessment of risk. This is one reason differences in the assessment of risk often arise within specific areas of application, making a direct comparison of the results difficult.

In practice, choosing the right method and the right tool for the analysis and evaluation of risk proves to be complicated. In recent years, a number of concepts, algorithms and tools have evolved from research, which have been especially designed to protect the ICT infrastructure and related systems. Since their historical background is settled in a business context, in these methods a quantitative risk assessment is usually performed based on monetary costs (e.g. EBIOS method and the aforementioned ISO / IEC 27005:2013 standard). In this context, most of the methods and tools just use the commonly known rule of thumb ‘risk = probability x potential damage’. Depending on the applied method, the terms and scales for the assessment of the probabilities as well as the potential damage are predefined (such as in the NIST policy or in the Mehari method).

In order to structure the process of risk assessment, various attempts have been made to use a Bayesian approach for determining threat probabilities. For example the OCTAVE method is based on subjectively estimated probabilities and thus can be understood as an apriori distribution with regards to the Bayesian approach. The OCTAVE method uses UML as a

modelling language and represents a comprehensive collection of tools and best practice methods for risk management. The 'BowTie' is a traditional widely used qualitative risk analysis method. The CORAS method allows the integration of several different risk assessment processes, whereas the identification of the probability of an attack is not done automatically but apriori to any risk assessment.

Contrary to the aforementioned general and IT-specific guidelines for risk management, security and risk management in various sectors emphasise different aspects in the RM methods. For example, the maritime sector traditionally lays a big emphasis on physical and object security. In particular, the International Ship and Port Facility Security (ISPS) Code define a set of measures to enhance the security of port facilities and ships. It is only this year that IMO published RM guidelines for the cyber assets of ships.

A sole focus on physical security is not sufficient any more in any sector due to the digitalisation and security of the cyber-physical systems becoming equally important. Thus RM need to cover all aspects. In this section we will present the main RM methodologies in terms of their main characteristics, usability, resources needed, standards applies and implementation aspects (supported by tools).

As explained in section 2.3, there are three options for the risk management analysis of methodologies.

Option 1: Methodology is used to achieve conformance to a standard (referencing in part or in whole to a certain standard and its requirements).

Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) Risk Manager

EBIOS Risk Manager is an information security risk management method, created under the French General Secretariat of National Defence, consistent with ISO 31000 and ISO/IEC 27005, and enables the risk management requirements of ISO/IEC 27001 to be met.

- It allows to:
    - establish the context (objectives, scope, critical and supporting assets on which they are based, etc.) and deal with standard and accidental risks by assessing compliance with the rules to which organisations have committed themselves;
    - assess targeted and sophisticated risks:
        - by studying and reconciling the points of view of the attacker (sources of risk) and the defender (feared events, sources of risk and their intended objectives);
        - by successive refinements (strategic scenarios studying the possible attack paths of the sources of risk through the ecosystem of stakeholders, and operational scenarios studying in detail the attack chains that allow them to be implemented in practice);
        - estimating their severity and likelihood;
    - deal with them in a proportionate manner, allowing the various components of the risks identified to be dealt with as the studies are carried out and completing the coverage of the risks in a coherent manner through an action plan;
    - accept the residual risks through a decision informed by the previous steps;
    - communicate risks, as it is participatory and involves several stakeholders (management, business, IT, security, legal, communication, etc.), and provide intelligible results to the recipients of the studies;

    - monitor and review risks as a principle of continuous improvement, by identifying the risks to be monitored and by providing for the conditions for updating the studies.
- More than a method, it is a methodology used as a toolbox whose terminology, techniques, sequence, knowledge bases and manner of presenting the results will be adjusted according to the object of the study (an entire organisation, a specific system, a technical component, etc.) and its context.

Method for the Harmonised Analysis of Risk (MAGERIT)

Magerit is an open methodology for risk analysis and management developed by the Spanish Higher Council for Electronic Government and offered as a framework and guide to the public administration. It is the answer to the increasing dependency of public and private organisations on information technologies to fulfil their mission and reach their business objectives.

Magerit users undertake the responsibility running the risk analysis process via workshops and interviews, with specific representatives of the organisation participating only in specific phases of the assessment process. It is compliant with ISO/IEC 27005, covers all the requirements defined by the ISO/IEC 27001, and conforms with the code of implementation of an ISMS specified by ISO/IEC 27002:2005.

Option 2: Methodology is given as a standard and can be used to achieve conformance to a standard and its requirements.

NIST 800-30 Methodology

NIST 800-30 is a free guide that provides a foundation for the development of an effective risk management programme, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems. The ultimate goal is to help mostly large scale organisations (such as governmental agencies and large companies) to better manage risks associated with IT-related missions.

The method is compliant with the ISO/IEC 27001.

Option 3: Methodology is a set of good practices but not related to any standard and not used to achieve conformance.

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Method

OCTAVE is a free of charge approach to evaluations of information security risk that is comprehensive, systematic, context-driven, and self-directed. The approach is embodied in a set of criteria that define the essential elements of an asset-driven evaluation of an information security risk.

CCTA Risk Assessment and Management Methodology (CRAMM)

CRAMM is a method that an analyst or group of analysts may use to evaluate the security and risk level of an organisation by analysing and combining the diverse knowledge distributed in the local corporate environment. The computational method and technique that has been adopted by CRAMM for the correlation and the determination of the results is quite primitive and is based on a qualitative approach. CRAMM complies with the rules and obligations imposed by the ISO/IEC 27001 standard.

IT-Grundschutz

IT-Grundschutz has been developed by the Federal Office for Information Security in Germany. IT-Grundschutz provides a configuration for the establishment of an integrated and effective IT security management. The method, before starting the risk analysis, involves a basic security check to verify the security measures that have been implemented. Risk assessment identifies the threats which have not been avoided by the measures, such as residual threats.

These threats can be eliminated by additional security measures. In this way, risk will be reduced to an acceptable level. IT-Grundschutz adopts a qualitative risk analysis approach that is associated with a primitive computational technique for the analysis and correlation of the assessment information. The method is compliant with ISO/IEC 27001 as it addresses the defined requirements as well as being suitable for the implementation of the ISMS process described in ISO/IEC 27002.

MEHARI

MEHARI is a free of charge qualitative risk analysis and management method developed by CLUSIF (Club for the Security of Information in France/Club de la Sécurité de l'Information Français). MEHARI provides a consistent methodology, with appropriate knowledge bases such as manuals and guides that describe the different modules (stakes, risks, vulnerabilities) that has been designed to assist people involved in security management (CISOs, risk managers, auditors, CIOs), in their various tasks and actions. The methodology is suitable for the implementation of the ISMS process described by ISO/IEC 27001.

Information Security Assessment and Monitoring Method (ISAMM)

ISAMM is a quantitative type of risk management methodology that can be applied by various organisations such as governmental agencies, large companies and small and medium size enterprises. ISAMM is compliant with ISO/IEC 27002 and provides maximal support of the ISO/IEC 27001 ISMS standard. It is also supported by a freeware tool.

4.2 OTHER SYSTEMS AND TOOLS SUPPORTING RM

Baldrige Cybersecurity Excellence Builder (BCEB) is a self-assessment tool to help organisations better understand the effectiveness of their cybersecurity risk management efforts and identity opportunities for improvement in the context of their overall performance.

Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures. It is a list of publicly disclosed computer security flaws with a CVE ID number assigned by a CVE numbering authority (CNA). There are about 100 CNAs, representing major ICT vendors, security companies and research organisations. MITRE also issues CVEs directly. A single complex ICT product, such as an operating system, can accumulate many CVEs.

Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS is well suited as a standard measurement system for industries, organisations and governments that need accurate and consistent vulnerability severity scores.

Security Content Automation Protocol (SCAP) is a synthesis of interoperable specifications derived from community ideas. This site contains information about both existing SCAP specifications and emerging specifications relevant to NIST's security automation agenda.

OWASP threat modelling tool is an open source tool that works to identify, communicate and understand threats and mitigations within the context of protecting something of value. Threat modelling can be applied to a wide range of things, including software, applications, systems, networks, distributed systems, things in the Internet of things, business processes, etc.

Factors Analysis in Information Risk (FAIR Privacy) is a quantitative privacy risk framework based on FAIR (Factors Analysis in Information Risk). FAIR Privacy examines personal privacy risks (to individuals), not organisational risks. Included in this tool is a PowerPoint deck illustrating the components of FAIR Privacy and an example based on the US Census. In addition, an Excel spreadsheet provides a powerful risk calculator using Monte Carlo simulation.

SRAQ Online Risk Calculator adopts a technical approach to RA; it covers four areas: identification of threats; development of system diagrams; recommendation of controls; creation of risk treatment plan.

Vulnerability registers and databases underpin the success of risk assessment which relies on these registers and databases and on the formats, metrics and procedures used in these registers and databases. They play an important role in the assessment and management of risk since they provide a unique identifier for each vulnerability, a structured and machine-readable format for the information and, typically, a number of references to fixes and patches. There are global registers such as MITRE CVE, NVD and CNNVD as well as national and commercial registries but no EU registry.

Sector specific prototypes for RM tools have been developed in various EC H2020 projects. These include the following.

CYSM emphasises the protection of port facilities, based on the provision of a dynamic risk management methodology for ports' CII considering their physical-cyber nature. It implements ISO 27001, ISO27005 and ISPS. The CYSM RA tool is based on a set of interactive and collaborative technologies.

MEDUSA focuses on the protection of the port supply chain. It defines a methodological approach to the identification of the multi-order dependencies of security incidents and risks, within the scope of multi-sector cross-border scenarios. It is reflected in the provision of support for ISO28000. MEDUSA is based on a set of visualisation tools and techniques to model and simulate the supply chain scenarios of ports.

MITIGATE enhances CYSM and Medusa towards protecting port facilities within the scope of interacting supply chains. MITIGATE adopts an evidence-driven maritime supply chain risk assessment model in order to capture and deal with cascading effects risks, threats and vulnerabilities, associated with the ICT-based maritime supply chain. It implements ISO 27001, ISO27005 and IOS28000 and incorporates a set of ICT technologies, including semantic web technologies (for ontology management, context management and profiling), cloud computing and BigData and crowd-sourcing technologies (i.e. in order to collect and analyse open information from public resources)

Cyberwatching Cyber Risk Temperature Tool is a tool developed for SMEs so they can easily identify threats and estimate their risks.

RESISTO implements an innovative decision support system to protect communication infrastructures from combined cyber-physical threats exploiting the Software De-fined Security model on a suite of state-of-the-art cyber-physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services.

FINSEC is a tool box that can be used by the financial sector. It implements an RA methodology based on the enhancement and integration of various existing tools for anomaly detection, AI CCTV analytics, risk assessment engines, collaborative analysis and management of risk.

There are global registers such as MITRE CVE, NVD, CNNVD. Many MSs have their own registries (national and regional) that are not connected or interoperable as has been realised

through an on-going study by ENISA on 'Vulnerability Disclosure Policies and Vulnerability Databases'. Moreover, there is no EU registry that all EU vendors can use to report new vulnerabilities. The national and regional registries are neither interoperable nor connected.

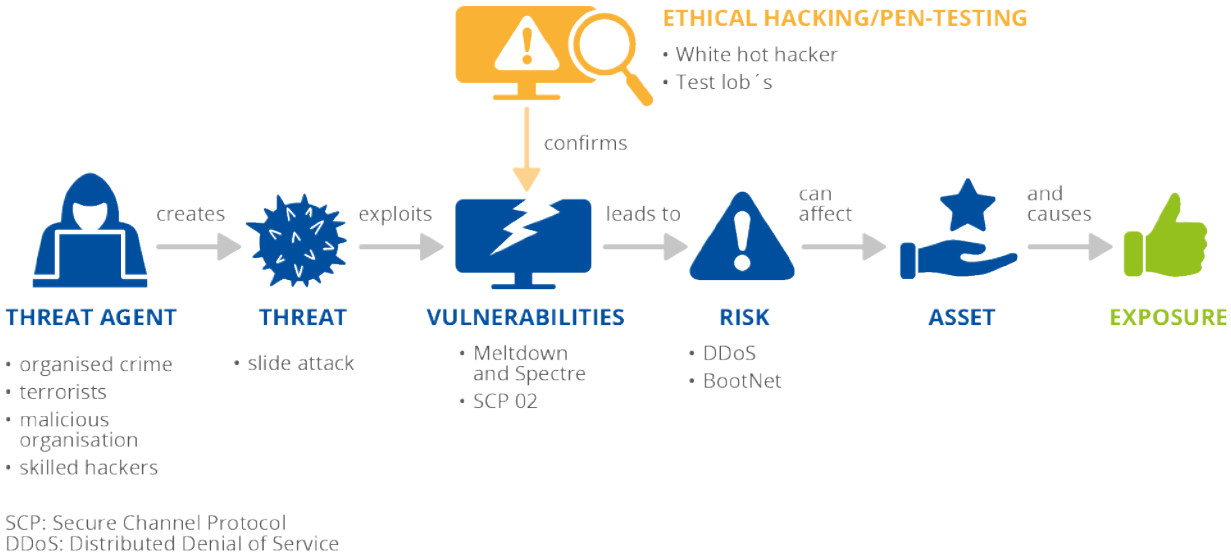
4.3 PRACTICAL USE OF STANDARDS AND METHODOLOGIES

Risk management standards and methodologies can be used for several purposes in an entity:

- Setting up or reinforcing a management process for the digital risk within an organisation,
- Assessing and treating the risks relating to a digital project, in particular with the aim of a security accreditation,
- Defining the level of security to be achieved for a product or service according to its particular uses and the risks to be countered, from the perspective of certification or accreditation for example.

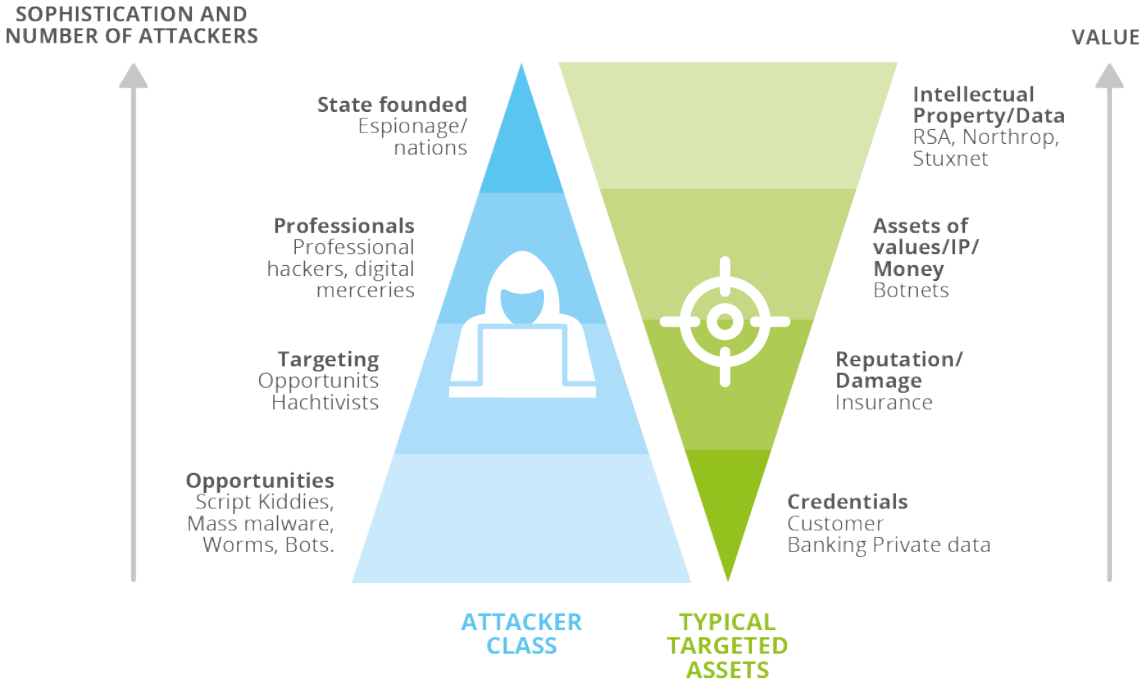
Before going on to the different steps of a practical implementation, it is important to understand the two main actors of the ICR possible risks, **threat agent and the asset**

1) The flow from threat agent to exposure of the asset



This diagram illustrates the various steps and causal relationship between the threat agent and the exposure of the asset, which is commonly known as a 'cyberattack'. The risk management and the associated methodology and tools are a set of requirements to be followed to estimate the level of risk that an entity is facing.

2) The threat agents can have different aspects and levels, depending on the value of the targeted assets.



It is interesting to see the evaluation of bank branches in the 1980s. The bank offices had several security functions that people had to go through before being able to enter the office. The asset to protected was the physical money. The banks performed risk analysis and realised that the only asset to be protected was the physical money and so they removed it from the hands of the employees. Now you can enter in any bank without going through any security functions as the physical money is managed by the ATM and bank employees don't have access to it.

This example illustrates why it is important to first identify the assets that are to be protected. If there is no asset then there is no risk.

The necessary steps to be conducted by any entity when starting its risk analysis can be summarised as below):

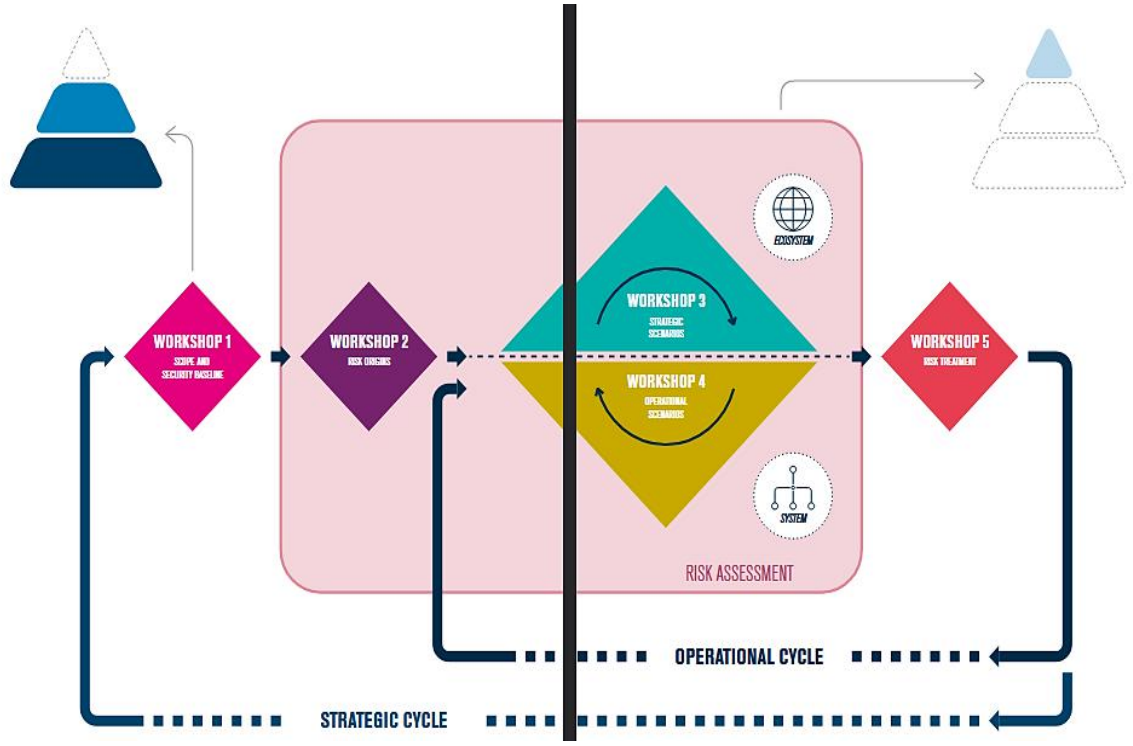
- Item 1: Identification of the critical assets (data, material, place, people);
- Item 2: Identification of the threats of these critical assets;
- Item 3: Definition of the occurrence and the importance of this threats to calculate a rate of risk;
- item 4: Decision on risk mitigation (reduce, accept, transfer);
- Item 5: Planification of business continuity plan and business resumption plan;
- Item 6: Definition of the IT cartography or the product usage environment.

In order to perform these six steps, the practical use of the ISO/IEC 27005 Risk Management Standard associated with the EBIOS RM assessment methodology can be applied. As the EBIOS Risk Management Assessment methodology[9] is based on the ISO/IEC 27005 and fully compliant, the entity does not have to know the ISO/IEC 27005 standard to perform its Risk mitigation analysis.

The EBIOS RM methodology adopts an iterative approach that revolves around five workshops.

[9] https://www.ssi.gouv.fr/uploads/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf - all subsequent images that relate to EBIOS RM are derived from this document, published by ANSSI

Figure 1 — An iterative approach in five workshops - Source ANSSI

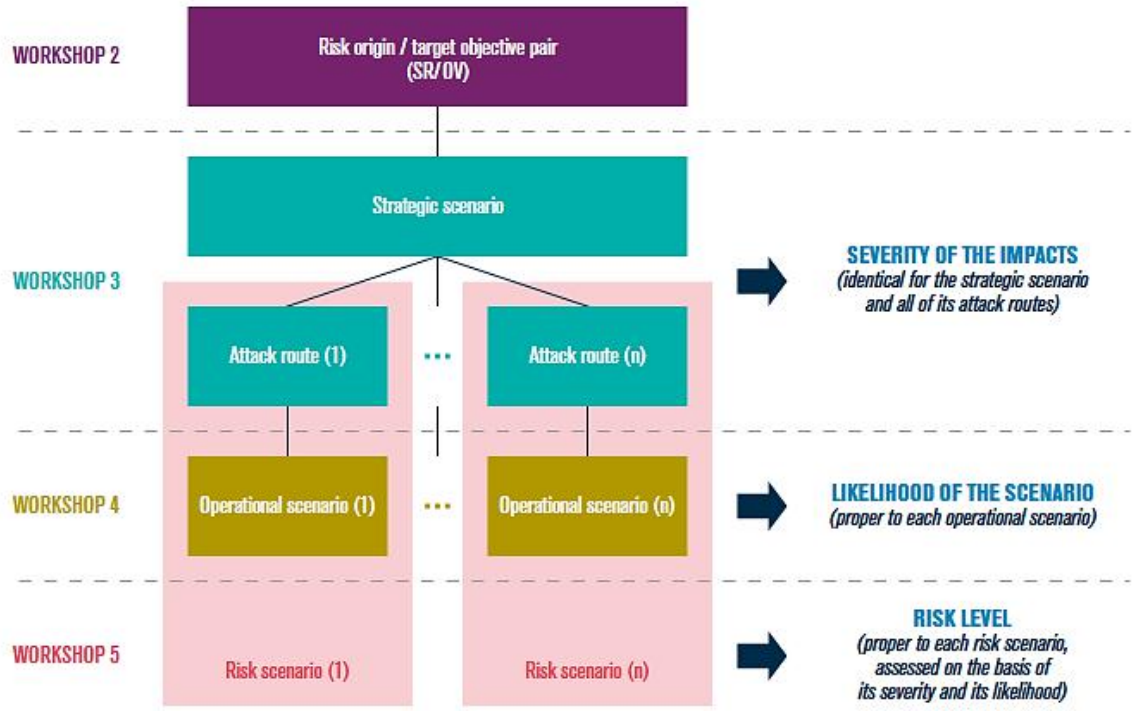


WORKSHOP 1 **Scope and security baseline**	The first workshop aims to identify the studied object, the participants in the workshops and the timeframe. During this workshop, you will list the missions, business assets and supporting assets related to the studied object. You identify the feared events associated with the business assets and assess the severity of their impacts. You also define the security baseline.
WORKSHOP 2 **Risk origins**	In the second workshop, you identify and characterise the risk origins (RO) and their high-level targets, called target objectives (TO). The RO/TO pairs deemed the most relevant are selected at the end of this workshop. The results are formalised in a mapping of the risk origins.
WORKSHOP 3 **Strategic scenarios**	In workshop 3, you will get a clear view of the ecosystem and stablish a mapping of the digital threat of the latter with respect to the studied object. This will allow you to construct high-level scenarios, called strategic scenarios. They represent the attack paths that a risk origin is likely to take to reach its target. These scenarios are designed at the scale of the ecosystem and the business assets of the studied object. They are assessed in terms of severity. At the end of this workshop, you can already define the security measures on the ecosystem.
WORKSHOP 4 **Operational scenarios**	The purpose of workshop 4 is to construct technical scenarios that include the methods of attack that are likely to be used by the risk origins to carry out the strategic scenarios. This workshop adopts an approach similar to the one in the preceding workshop but focuses on critical supporting assets. You then assess the level of likelihood of the operational scenarios obtained.

	NOTE: 1) Workshops 3 and 4 are naturally applied during successive iterations. 2) Workshops 2, 3 and 4 make it possible to assess the risks, which constitute the last stage of the digital risk management pyramid. They use the security baseline according to different attack paths, which are relevant with regards to the threats considered and in a limited number in order to facilitate the analysis.
WORKSHOP 5 **Risk mitigation**	The last workshop consists in creating a summary of all of the risks studied in order to define a risk mitigation strategy. The latter is then broken down into security measures written into a continuous improvement plan. During this workshop, you establish a summary of the residual risks and define the framework for monitoring risks.

This series of five iterative workshops is summarised here below:

Figure 2: Link between the various workshop – source EBIOS RM - ANSSI



To support and implement this methodology you can use a simple table file. Some software editors also provide dedicated software that is available in Software as a Service mode or local mode.

5. RESULTS OF THE ANALYSIS

This section analyses the gaps and overlaps between the risk management standards determined in section 4.1.5.

When analysing the documents discussed earlier, the distinction between risk management standards and risk management methodologies becomes quite obvious. The relevant standards are:

- ISO/IEC 27005 – Information security risk management,
- ISO 31000 – Risk management guidelines,
- BSI 7799-3 – Guidelines for information security risk management,
- NIST SP 800-39 – Managing information security risk,
- BSI Germany Standard 200-3 – Risk analysis based on IT-Grundschutz.

Their analysis in this section is performed from various perspectives:

- concepts, terms and definitions,
- risk criteria,
- areas of application,
- ICT,
- level of application,
- European vs international technical specifications,
- EU legislation vs standards.

Concepts, terms and definitions

All the identified risk management standards have influenced each other over the years. The concepts, terms and definitions related to risk management outlined in ISO 31000 have been incorporated in all of these other documents in more or less the same way.

Slight deviations exist depending whether the risk management standards analysed are more related to or in support of management system standards based on ISO Directives or those based on a risk management framework according to ISO 31000. This difference becomes quite obvious when reading the diverging definitions of risk, but this distinction has no real-life implications and can be viewed as a rather academic issue.

The risk management methodologies and tools do diverge to a much greater extend from each other. This can mostly be attributed to the fact that these methodologies and tools have been developed by different entities addressing different audiences and their needs. Not every methodology or tool is universally applicable to any type or size of organisation and its scope.

In the ENISA report *Methodology for Sectoral Cybersecurity Assessments* 2021 an overview of terms is provided, along with an interpretation of the meaning of each term according to the normative references found in ISO/IEC 270xx. In addition, how these definitions should be understood and used in the context of the specification of security and assurance is explained.

Risk Criteria

All risk management standards recommend the determination of risk criteria, although no recommendation or requirement regarding the criteria themselves or the necessary levels or threshold values are stated. According to the risk management standards, this remains a task for the organisation implementing risk management.

The risk management methodologies and tools may have outlined these risk criteria – including the levels and threshold values – within their content. Depending on the audience for a methodology or tool, these criteria can be defined exactly for the specific area of application, such as a specific business sector.

The various RA methodologies adopt different measurement and scales so as a result risk levels estimates cannot be compared. These differences lead to selecting and implementing different controls (some of them costlier that others) to mitigate the same risks. This problem affects certification efforts as well. CVSS3.0 is being used broadly for scoring the severity of vulnerabilities; however, it has not been adopted by all stakeholders.

Areas of application

All the risk management standards that have been identified can be applied by any organisation in any business sector as these standards provide guidance on the framework for risk management.

The situation is similar for organisations implementing risk management in the context of a management system when seeking conformance to a management system standard.

Some methodologies and tools may be applicable only to a specific business sector. Others also address ICT-risk from a cross-sector perspective.

The transversal standards intend to cover a large set of domains by being as generic and reusable as possible. This is the case of standards developed by ISO/IEC JTC1/SC27 (ISO/IEC 27000 family, ISO/IEC 15408/18045) or by CEN CENELEC EN 17640 FITCEM or ETSI EN 303 645. Despite this fact it appears that for specific domains (automotive, aeronautics and space, energy, sustainable industry, supply chain etc.), these standards are not sufficient and must be supplemented with additional security requirements, and evaluation and assessment methods. This can be due to specific features, regulations, user requirements or technology constraints.

ICT

There are many standards on ICT security (e.g. ISO/IEC 11770-3:2021) that provide accurate technical information to ensure the security of ICT mechanisms and also several sector-specific standards due to ISO /IEC 27002 Code of Practice for information security controls, e.g. ISO/IEC 27011. They support managing ICT security risks by offering appropriate technology and related mechanisms but they are not risk management standards.

ETSI TS T02 165-1 (2017) is a technical specification which defines a method for analysing the risks of information and communications technology (ICT) systems using the threat, vulnerability and risk analysis (TVRA) methodology. Primarily, this is a guidance for analysing threats applicable to and vulnerabilities identified in a target of evaluation considered within the Common Criteria evaluation methodology (ISO/IEC 15408 family). But there is no equivalent standard considering ICT systems in a more general context.

There are several sector-specific standards due to ISO /IEC 27002 Code of Practice for information security controls, e.g. ISO/IEC 27011 (Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organisations) and ISO/IEC 27017 (Code of practice for information security controls based on ISO/IEC 27002 for cloud services). There are some standards applying risk management to technology, e.g. ISO 14971 (Medical devices — Application of risk management to medical devices) and ISO 17666 (Space systems — Risk management). But there is a gap due to the absence of a standard applying risk management to ICT devices, ICT services and ICT processes to support the assessment and treatment of corresponding risks.

The following results can be observed in several organisations:

1. Lack of coordination and alignment between the divisions responsible for business risk management or information security management and ICT staff regarding risk management;
2. Lack of conformity with regard to risk management language and the application of risk management between the divisions responsible for business risk management or information security management and ICT staff.

Level of application

As risk management standards only provide guidance on the framework, these standards can be used by the whole of a legal entity[10] from the perspective of its business, its services or products, or be limited to its IT-operation only.

Depending on the audience and the intended use of a methodology or tool, similar organisational levels can be addressed. Some tools cover all aspects of a management system – such as management system risks, strategic risk and operational risks – others only address operational risk for ICT-operations.

European vs international technical specifications

Out of the five risk management standards as determined, two are published by ISO, whereas three standards are published by individual countries. None of these publications have any legal basis throughout the European Union.

The situation poses similar problems regarding methodologies and tools.

Section 4.1.5 has identified ISO 31000 Risk Management Guidelines and ISO/IEC 27005 Information Security Risk Management as being the most relevant risk management standards in the international domain, providing basic principles and generic guidelines. Unlike many other international cybersecurity standards which have been adopted as European Norms, such adoption has not happened in these two cases; however ISO 31000 was, for example, adopted as a regional standard for Australia and New Zealand.

EU legislation versus standards

The EU's NIS directive uses its own definition of risk which is not aligned with any of the other definitions. For example, The definition of 'risk' is not uniform between the NIS directive and ISO/IEC 27001 and ISO/IEC 27005. This issue may be rather academic but it can also create some difficulties in bridging the regulatory context and the standardisation context.

[10] From the perspective of management system standards, the organisation is always related to the scope of the management system – and its risk management – and the distinction between 'legal organisation' and 'IT-operation' is incorrect.

The risk-based approach is promoted in most of the recent efforts on digital legislation. As an example, the IA Act defines four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk. To classify these four levels, an agreed quotation methodology should be developed and, as of today, no standard is available nor is one in preparation.

6. RECOMMENDATIONS

Basing on the analysis provided in section 5, we propose the following recommendations on the use of risk management standards for various groups of stakeholders.

6.1 EU POLICY MAKERS

Recommendation 1:

EU policy makers should use risk management standards that have already been adopted in future regulatory publications.

Note: This requires the successful implementation of recommendation 8.

Recommendation 2:

EU policy makers should make particular risk assessment methodologies or tools mandatory for specific sectors, where and when necessary.

Recommendation 3:

When no risk management standard or risk assessment methodology or tool is appropriate for a specific sector, EU policy makers should issue a request for standardisation to ESOs to cover this need.

As an example – a European standard for a methodology for the assessment of ICT security is missing. Such a European standard would allow a coherent approach to be made to comply with the risk management obligation set out in different existing and upcoming cybersecurity pieces of legislation. This methodology should be based on the ISO/IEC 27005 Information security risk management and ISO/IEC ISO.IEC 31000 – Risk management guidelines.

Recommendation 4:

In the context of the Cybersecurity Act, one of the crucial actions should consist in verifying whether European standards to apply risk management to ICT devices, ICT services and ICT processes, which aim to support the assessment and treatment of corresponding risks, actually exist. Otherwise, the EU Policy makers should issue a request for standardisation to ESOs to cover this need.

Recommendation 5:

Cybersecurity education and practical skills need to be aligned and embedded in all educational stages (from early childhood to lifelong learning) and during the whole professional life. All educational enterprises in the MSs and all EU citizens from all sectors (e.g. health, government, transport, finance, defence) need to have the opportunity to practice in national or clustered EU cyber ranges to assess their skills. Risk management, based on the recognised standards, should become one of the main topics of these activities.

Recommendation 6:

An ad hoc working group should be set up (preferably by ENISA) to determine some criteria to define the levels of risks mentioned in European legislation (e.g. Artificial Intelligence Act). This ad hoc working group should provide the necessary risk tools to compute the estimation of the risk and to classify the results accordingly to the levels identified.

6.2 EUROPEAN SDOS

Recommendation 7:

As identified earlier, security concepts (units of knowledge consisting of unique characteristics), terms (verbal designations of the concepts), definitions (unique descriptive statements of the concepts that identify them uniquely) and relations between concepts in different risk assessment standards deviate among themselves as used by various SDOs. Further interpretation efforts are needed for all risk assessment and risk management standards that appear in this document.

The SDOs are encouraged to use unified concepts, terms and definitions.

The concept approach, developed by the ISO Technical Committee TC37 Language and Terminology, can be adopted where one term corresponds to one concept and only one concept corresponds to one term.

Recommendation 8:

There is no existing European standard for a methodology to assess ICT security available at the European level, creating some issues in referencing applicable standards in EU legislation.

As described in chapter 4.2 there are several methodologies with different approaches.

Efforts should be undertaken to address these gaps.

Recommendation 9:

ESOs should adopt ISO/IEC 31000 and ISO/IEC 27005 as European Norms.

The benefits of such regional adoption in the case of European Norms include the facts that:

- harmonisation within Europe makes it easier to comply with European rules and regulations (stand-still on national work on the same topic);
- documents can be targeted at European needs;
- consensus building within Europe is easier than in the global context.

The potential adoption of ISO/IEC 31000 and/or ISO/IEC 27005 as European standards will help to harmonise European approaches to risk management.

Recommendation 10:

ETSI should harmonise its TS 102 165-1 with ISO 31000 and ISO/IEC 27005 to develop a standard covering risk management for ICT systems which is applicable to systems in a Common Criteria context as well as in risk management (asset-based approach) within the scope of an ISMS.

6.3 ENISA

Recommendation 11:

ENISA should publish, on a regular basis, an overview of endorsed risk management standards covering different domains and sectors.

Recommendation 12:

ENISA should publish an overview of endorsed methodologies and tools covering different domains and sectors.

Recommendation 13:

ENISA should encourage and support different disciplines and sectors to develop or advance work regarding their assessment of sector-discipline-specific risk and methodologies and tools for treating risk, in order to increase cooperation between stakeholders.

Recommendation 14:

ENISA should continue to work in close support with ESOs in fulfilling potential EU requests for standardisation related to the management of risk.

Recommendation 15:

ENISA should establish a mechanism for assisting EU institutions, bodies and agencies, EU Member States and private organisations regarding various aspects of risk management.

ANNEX A: INVENTORY OF RISK MANAGEMENT RELATED STANDARDS

This annex lists the standards and technical specifications related to risk management. A full table, including additional information (such as the interrelation with other documents, current version, website link and others is available for download separately from the ENISA website.

Name	Document reference	Document type	Document scope	Name of the publishing Organisation	Short description
Safety of machinery — General principles for design — Risk assessment and risk reduction	ISO 12100:2010	Standard	Guidelines	ISO	This international standard specifies basic terminology, principles and a methodology for achieving safety in the design of machinery. It specifies principles of risk assessment and risk reduction to help designers in achieving these objectives.
Bases for design of structures — General principles on risk assessment of systems involving structures	ISO 13824:2020	Standard	General risk assessment framework	ISO	This document specifies general principles of risk assessment for systems involving structures. The focus is on strategic and operational decision-making related to the design, assessment, maintenance and decommissioning of structures. This also includes formulation and calibration of related codes and standards. Systems involving structures can expose stakeholders at various levels in society to significant risks.
Medical devices — Application of risk management to medical devices	ISO 14971:2019	Standard	Guidelines	ISO	This document specifies terminology, principles and a process for risk management of medical devices, including software as a medical device and in vitro diagnostic medical devices. The process described in this document is intended to assist manufacturers of medical devices to identify the hazards associated with a medical device, to estimate and evaluate the associated

					risks, to control these risks, and to monitor the effectiveness of the controls.
Space systems — Risk management	ISO 17666:2016	Standard	Requirements	ISO	Defines the principles and requirements for integrated risk management on a space project.
Specification for security management systems for the supply chain	ISO 28001:2007	Standard	Requirements and guidance	ISO	Outputs resulting from this international standard will be the following: i) A Statement of Coverage that defines the boundaries of the supply chain that is covered by the security plan; ii) A Security Assessment that documents the vulnerabilities of the supply chain to defined security threat scenarios which also describes the impacts that can reasonably be expected from each of the potential security threat scenarios; iii) A Security Plan that describes security measures in place to manage the security threat scenarios identified by the Security assessment; iv) a training programme setting out how security personnel will be trained to meet their assigned security related duties.
Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 — Part 2: Guidelines for adopting ISO 28000 for use in medium and small seaport operations	ISO 28004-2:2014	Standard	Guidelines	ISO	ISO 28004-2:2014 identifies supply chain risk and threat scenarios, procedures for conducting assessments of risks and threats, and evaluation criteria for measuring the conformance and effectiveness of the documented security plans in accordance with ISO 28000 and the ISO 28004 series implementation guidelines.
Risk Management Guidelines	ISO 31000	Standard	Guidelines	ISO	ISO 31000:2018 provides guidelines on managing the risks faced by organisations. The application of these guidelines can be customised to any organisation and its context.
Risk management — Vocabulary	ISO Guide 73:2009	Guide/Guidance	Vocabulary	ISO	ISO Guide 73:2009 provides the definitions of the generic terms related to risk management. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and

					frameworks dealing with the management of risk.
Risk management – Vocabulary	ISO/DIS 31073	Standard	Vocabulary	ISO	This document provides the definitions of generic terms related to the management of risks faced by the organisation. It aims to encourage a mutual and consistent understanding of, and a coherent approach to, the description of activities relating to the management of risk, and the use of uniform risk management terminology in processes and frameworks dealing with the management of the risks faced by organisations.
Application of risk management for IT-networks incorporating medical devices — Application guidance — Part 2-7: Guidance for Healthcare Delivery Organizations (HDOs) on how to self-assess their conformance with IEC 80001-1	ISO/TR 80001-2-7:2015	Technical Report	Guidelines	ISO	This part of ISO/TR 80001 provides guidance for a healthcare delivery organisation (HDO) that wishes to self-assess its implementation of the processes of IEC 80001-1. This part of ISO/TR 80001 can be used to assess Medical IT-Network projects where IEC 80001-1 has been determined to be applicable
Health informatics — Information security management for remote maintenance of medical devices and medical information systems — Part 1: Requirements and risk analysis	ISO/TS 11633-1:2019	Technical Specification	Requirements and risk analysis	ISO	This document focuses on remote maintenance services (RMS) for information systems in healthcare facilities (HCFs) as provided by vendors of medical devices and health information systems. This document specifies the risk assessment necessary to protect remote maintenance activities, taking into consideration the special characteristics of the healthcare field such as patient safety, regulations and privacy protections. This document provides practical examples of risk analysis to protect the information assets of both HCF and RMS providers in a safe and efficient (i.e. economical) manner. These assets are primarily the information system itself and personal health data held in the information system.
Guidance on performing risk assessment in the design of onshore LNG installations including the ship to shore interface	ISO/TS 16901:2015	Technical Specification	Guidelines	ISO	This Technical Specification provides a common approach and guidance to those undertaking assessment of the major safety hazards as part of the planning, design, and operation of LNG facilities onshore and at the shoreline using risk-

					based methods and standards, to enable the safe design and operation of LNG facilities.
Risk management — Guidelines on using ISO 31000 in management systems	IWA 31:2020	IWA Workshop Agreement	Guidelines	ISO	This document gives guidelines for integrating and using ISO 31000 in organisations that have implemented one or more ISO and IEC management system standards (MSS), or that have decided to undertake a project implementing one or more MSS incorporating ISO 31000. This document explains how the clauses of ISO 31000 relate to the high level structure (HLS) for MSS.
Information security management systems — Overview and vocabulary	ISO/IEC 27000:2018	Standard	Vocabulary	ISO/IEC	ISO/IEC 27000:2018 provides an overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organisation (e.g. commercial enterprises, government agencies, and not-for-profit organisations).
Information security management systems — Requirements	ISO/IEC 27001:2013	Standard	Requirements	ISO/IEC	ISO/IEC 27001:2013 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation.
Security techniques — Code of practice for information security controls	ISO/IEC 27002:2014	Standard	Code of practice	ISO/IEC	ISO/IEC 27002:2013 gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s).
Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation	ISO/IEC 27004:2016	Standard	Guidelines	ISO/IEC	ISO/IEC 27004:2016 provides guidelines intended to assist organisations in evaluating the information security performance and the effectiveness of an information security management system in order to fulfil the requirements of ISO/IEC 27001:2013.
Security techniques — Information security risk management	ISO/IEC 27005:2018	Standard	Guidelines	ISO/IEC	This document provides guidelines for information security risk management. This document supports the general concepts specified in ISO/IEC 27001 and is designed to

					assist the satisfactory implementation of information security based on a risk management approach.
Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems	ISO/IEC 27006:2015	Standard	Requirements	ISO/IEC	ISO/IEC 27006:2015 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.
Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1	ISO/IEC 27013:2015	Standard	Guidelines	ISO/IEC	ISO/IEC 27013:2015 provides guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 for those organisations that are intending to either: i) implement ISO/IEC 27001 when ISO/IEC 20000-1 is already implemented, or vice versa, ii) implement both ISO/IEC 27001 and ISO/IEC 20000-1 together, iii) integrate existing management systems based on ISO/IEC 27001 and ISO/IEC 20000-1. ISO/IEC 27013:2015 focuses exclusively on the integrated implementation of an information security management system (ISMS) as specified in ISO/IEC 27001 and a service management system (SMS) as specified in ISO/IEC 20000-1.
Information technology — Organisational privacy risk management	ISO/IEC CD 27557	Standard	Requirements	ISO/IEC	Under development
Information technology — Security techniques — Security assessment of operational systems	ISO/IEC TR 19791:2010	Technical Report	Guidelines	ISO/IEC	This technical report provides guidance and criteria for the security evaluation of operational systems. It provides an extension to the scope of ISO/IEC 15408, by taking into account a number of critical aspects of operational systems not addressed in ISO/IEC 15408 evaluation. The principal extensions that are required address evaluation of the operational environment surrounding the target of evaluation, and the decomposition of complex operational systems into security domains that can be separately evaluated.

Information technology — Process assessment — Guidance for process risk determination	ISO/IEC TR 33015:2019	Technical Report	Guidelines	ISO/IEC	This document provides guidance on the application of the results of a process assessment for process risk determination.
Road vehicles — Cybersecurity engineering	ISO/SAE 21434:2021	Standard	Requirements	ISO/SAE	This document addresses the cybersecurity perspective in the engineering of electrical and electronic (E/E) systems within road vehicles. By ensuring appropriate consideration of cybersecurity, this document aims to enable the engineering of E/E systems to keep up with state-of-the-art technology and evolving attack methods.
Risk Management – Risk assessment techniques	IEC 31010:2019	Standard	Techniques	IEC	IEC 31010:2019 is published as a double logo standard with ISO and provides guidance on the selection and application of techniques for assessing risk in a wide range of situations. The techniques are used to assist in making decisions where there is uncertainty, to provide information about particular risks and as part of a process for managing risk. The document provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail.
Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software — Part 1: Application of risk management	IEC/DIC 80001-1	Standard	Requirements	IEC	This document specifies general requirements for organisations in the application of risk management before, during and after the connection of a health IT system within a health IT infrastructure, by addressing the key properties of safety, effectiveness and security whilst engaging appropriate stakeholders.
Fixed time cybersecurity evaluation methodology for ICT products	prEN 17640	Other	Evaluation Methodology	CEN-CLC	This document describes the cybersecurity evaluation methodology for ICT products. It is intended for use for all three assurance levels as defined in the Cybersecurity Act (i.e. basic, substantial and high). The methodology is comprised of different evaluation blocks including assessment activities that comply with the evaluation requirements of the CSA for the three levels. Where appropriate, it can be applied both to third party evaluation and self-assessment. It is expected that this methodology may be used by different

					candidate schemes and verticals providing a common framework to evaluate ICT products.
Information security management systems — Overview and vocabulary	EN ISO/IEC 27000:2020	Standard	Vocabulary	CEN-CLC	EN ISO/IEC 27000 provides an overview of information security management systems (ISMS). It also provides terms and definitions commonly used in the ISMS family of standards. This document is applicable to all types and sizes of organisation (e.g. commercial enterprises, government agencies, not-for-profit organisations).
Information security management systems — Requirements	EN ISO/IEC 27001:2017	Standard	Requirements	CEN-CLC	EN ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation.
Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines	EN ISO/IEC 27701:2021	Standard	Requirements	CEN-CLC	This document specifies requirements and provides guidance for establishing, implementing, maintaining and continually improving a privacy information management system (PIMS) in the form of an extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy management within the context of the organisation.
Security techniques — Code of practice for information security controls	EN ISO/IEC 27002:2017	Standard	Code of practice	CEN-CLC	EN ISO/IEC 27002 gives guidelines for organisational information security standards and information security management practices including the selection, implementation and management of controls taking into consideration the organisation's information security risk environment(s)
Requirements for bodies providing audit and certification of information security management systems	EN ISO/IEC 27006:2020	Standard	Requirements	CEN-CLC	EN ISO/IEC 27006 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1 and EN ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements	TS 103 701	Other	Evaluation Methodology	ETSI	The present document specifies a methodology for the assessment of conformance for consumer IoT devices, their relation to associated services and corresponding relevant processes against ETSI TS 103 645 [1] or ETSI EN 303 645 [2], addressing the mandatory and recommended provisions as well as the conditions and complements of ETSI TS 103 645 [1]or ETSI EN 303 645 [2] by defining test cases and assessment criteria for each provision.
CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability and Risk Analysis (TVRA).	ETSI TS 102 165-1	Technical Specification	Technical specification	ETSI	The current document defines a method primarily for use by developers of ETSI standards in undertaking an analysis of the threats, risks and vulnerabilities of an information and communications technology (ICT) system
Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat, Vulnerability and Risk Analysis	ETSI TR 187 002	Technical Report	Technical report	ETSI	The present document presents the results of the threat vulnerability risk analysis (TVRA) for the NGN.
Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy	SP 800-37 Rev.2	Guide/Guidance	Guidance	NIST	The Risk Management Framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system's development life cycle. The risk-based approach to control selection and specification considers effectiveness, efficiency, and constraints due to applicable laws, directives, executive orders, policies, standards or regulations.
Managing Information Security Risk: Organisation, Mission, and Information System View	SP 800-39	Guide/Guidance	Guidelines	NIST	The purpose of Special Publication 800-39 is to provide guidance for an integrated, organisation-wide programme for managing information security risk to organisational operations (i.e. mission, functions, image, and reputation), organisational assets, individuals, other organisations and the nation resulting from the operation and use of federal information systems.

Supply Chain Risk Management Practices for Federal Information Systems and Organisations	SP 800-161	Guide/Guidance	Guidelines	NIST	The purpose of this publication is to provide guidance to federal agencies on identifying, assessing, selecting and implementing risk management processes and mitigating controls throughout their organisations to help manage ICT supply chain risks.
Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	NISTIR 8276	Other	Best practices	NIST	This document provides the ever-increasing community of digital businesses a set of key practices that any organisation can use to manage cybersecurity risks associated with their supply chains.
Integrating Cybersecurity and Enterprise Risk Management (ERM)	NISTIR 8286	Guide/Guidance	Guidelines	NIST	This document is intended to help individual organisations within an enterprise improve their cybersecurity risk information, which they provide as inputs to their enterprise's ERM processes through communications and risk information sharing. By doing so, enterprises and their component organisations can better identify, assess and manage their cybersecurity risks in the context of their broader mission and business objectives.
Risk analysis based on IT-Grundschutz	BSI-Standard 100-3	Other	Methodology	BSI (Germany)	The methodology demonstrates how the threats listed in the IT-Grundschutz catalogues can be used to carry out a simplified analysis of risks for information processing.
IT-Grundschutz Methodology	BSI-Standard 100-2	Other	Methodology	BSI (Germany)	The IT-Grundschutz Methodology is a BSI methodology for effective management of the information security that can be easily adapted to the situation of a specific organisation. This method provides both a methodology for setting up a management system for information security and a comprehensive basis for assessing risks, monitoring the existing security level, and implementing the appropriate information safeguards.

CACAO Security Playbooks Version 1.0	CACAO-Security-Playbooks-v1.0	Other	Methodology	OASIS	To defend against threat actors and their tactics, organisations need to identify, create, document, and test detection, investigation, prevention, mitigation and remediation steps. These steps, when grouped together form a cyber security playbook that can be used to protect organisational systems, networks, data and users. This specification defines the schema and taxonomy for collaborative automated courses of action for operations (CACAO) and security playbooks and how these playbooks can be created, documented and shared in a structured and standardised way across organisational boundaries and technological solutions. It defines the following classes of objects: playbooks (section 4), workflow steps (section 5), commands (section 6), targets (section 7), extensions (section 8), and data markings (section 9).
CSAF Common Vulnerability Reporting Framework (CVRF) Version 1.2.	CVRF-v1.2	Other	guidelines, methodology, data specification	OASIS	A standard language supporting creation, update, and interoperable exchange of security advisories as structured information on products, vulnerabilities and the status of impact and remediation among interested parties. The term Security Advisory is used to describe any notification of security issues in products of and by providers. The focus is on the security aspect impacting (or not impacting) specific combinations of products, platforms, and versions. Information on the presence or absence of work-arounds is also considered part of the security issue. It addresses security advisories from anyone providing a product, i.e. developers or maintainers of information system products or services. This includes all authoritative product vendors, product security incident response teams (PSIRTs), and product resellers and distributors, including authoritative vendor partners.

Open Command and Control (OpenC2) Language Specification Version 1.0	OpenC2-Lang-v1.0	Other	Methodology, data specification	OASIS	A concise and extensible language to enable machine-to-machine communications for purposes of the command and control of cyber defence components, subsystems and/or systems in a manner that is agnostic of the underlying products, technologies and transport mechanisms. OpenC2 is a suite of specifications that enables command and control of cyber defence systems and components, typically using a request-response paradigm. OpenC2 allows the application producing the commands to discover the set of capabilities supported by the managed devices. These capabilities permit the managing application to adjust its behaviour to take advantage of the features exposed by the managed device. The capability definitions can be easily extended in a non-centralised manner, allowing standard and non-standard capabilities to be defined with semantic and syntactic rigor.
Open Command and Control (OpenC2) Profile for Stateless Packet Filtering Version 1.0	OpenC2-SLPF-v1.0	Other	Methodology	OASIS	Open Command and Control (OpenC2) is a concise, extensible language enabling command and control of cyber defence components. Stateless packet filtering is a cyber defence mechanism that denies or allows traffic based on static properties of the traffic, such as address, port, protocol, etc. This profile defines the actions, targets, specifiers and options that are consistent with version 1.0 of the OpenC2 Language Specification in the context of stateless packet filtering (SLPF). An actuator profile for OpenC2 that specifies the set of actions, targets, specifiers and command arguments integrates SLPF functionality with the Open Command and Control (OpenC2) Command set.
Specification for Transfer of OpenC2 Messages via HTTPS Version 1.0	OpenC2-HTTPS-v1.0	Other	Methodology	OASIS	Open Command and Control (OpenC2) is a concise, extensible language enabling command and control of cyber defence components. Stateless packet filtering is a cyber defence mechanism that denies or allows traffic based on static properties of the traffic, such as

					address, port, protocol, etc. This document specifies the use of hypertext transfer protocol (HTTP) over transport layer security (TLS) as a transfer mechanism for OpenC2 messages. The specification provides guidance to the OpenC2 implementation community when using HTTPS for OpenC2 message transport. It includes guidance for the selection of TLS versions and options suitable for use with OpenC2.
Static Analysis Results Interchange Format (SARIF) Version 2.1	SARIF-v2.1.0	Other	Methodology, data specification	OASIS	SARIF is included because of its potential relevance to risk assessment. Software developers use a variety of analysis tools to assess program qualities such as correctness, security, vulnerability, performance, compliance with contractual or legal requirements, etc. SARIF defines a standard format for the output of static analysis tools to enable aggregation, analysis, and sharing of results. The standard defines a format for the output of static analysis tools, in order to capture the range of data produced by commonly used static analysis tools, enable data interchange, reduce cost and complexity, and capture information useful for assessing a project's compliance with corporate policy or certification standards.
STIX Version 2.1	STIX-v2.1	Other	Methodology, data specification	OASIS	A language and serialisation format used to exchange cyber threat intelligence (CTI), STIX enables CTI-sharing in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

TAXII Version 2.1	TAXII-v1.1.1-Overview	Other	Methodology	OASIS	TAXII is an application layer protocol for the communication of cyber threat information in a simple and scalable manner. This specification defines the TAXII RESTful API and its resources along with the requirements for TAXII client and server implementations. Trusted Automated eXchange of Indicator Information (TAXII™) defines a set of services and message exchanges that, when implemented, enable sharing of actionable cyber threat information across the organisation and product or service boundaries. TAXII, through its member specifications, defines concepts, protocols and messages to exchange cyber threat information for the detection, prevention, and mitigation of cyber threats. TAXII is not an information sharing initiative or application and does not attempt to define trust agreements, governance, or non-technical aspects of cyber threat information sharing.
Enterprise Risk Management — Integrated Framework	COSO ERM	Guide/Guidance	Guidance	COSO Committee of Sponsoring Organisations of the Treadway Commission	The Framework defines the essential components of enterprise risk management, discusses key ERM principles and concepts, suggests a common ERM language, and provides clear direction and guidance for enterprise risk management.
Systems and software engineering — Life cycle processes — Risk management	ISO/IEC/IEEE 16085:2021	Guide/Guidance	Guidelines	Other	This document provides information on how to design, develop, implement, and continually improve risk management in a systems and software engineering project throughout its life cycle.
Risk management - Principles and guidelines	AS/NZS ISO 31000:2009	Standard	Risk management	Other	Providing principles and generic guidelines on risk management, this standard can be used by any public, private or community enterprise, association, group or individual, and is not specific to any industry or sector. It can be applied throughout the life of an organisation, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets. Although the standard provides generic guidelines, it is not intended to promote

					uniformity of risk management across organisations. The design and implementation of risk management plans and frameworks will need to take into account the varying needs of a specific organisation, its particular objectives, context, structure, operations, processes, functions, projects, products, services or assets and specific practices employed.
Security for industrial automation and control systems–Part 3-2: Security risk assessment for system design	ISA/IEC 62443-3-2	Standard	Techniques	Other	This document strives to define a set of engineering measures that will guide an organisation through the process of assessing the risk of a particular industrial automation and control system (IACS) and enable it to identify and apply security countermeasures to reduce that risk to tolerable levels.
OWASP Risk Rating Methodology	OWASP Risk Assessment Framework	Other	Risk Assessment Framework	OWASP	The OWASP Risk Assessment Framework consists of static application security testing and risk assessment testers able to analyse and review their code quality and vulnerabilities.

ANNEX B: ANALYSIS OF EIDAS REGULATION

We present below an example of how ICT risk and risk management are treated by analysing the existing eIDAS regulation (Electronic Identification and Trust Services for Electronic Transactions - Regulation (EU) No 910/2014).

eIDAS items	Electronic Identification and Trust Services for Electronic Transactions - Regulation (EU) No 910/2014	Means
Identification schemes – Mutual recognition	Recital (20): cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and **security appropriate to the degree of risk**. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.	Risk management performed by peer reviews
Trust Service Providers	Recital (32): it should be incumbent on all trust service providers to apply good security practice appropriate to **the risks related to their activities** so as to boost users' trust in the single market.	Apply good security practices
Data protection handle by electronic registered delivery service	Recital (36): 'electronic registered delivery service' means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the data transmitted, including proof of sending and receiving the data, and that protects transmitted data against **the risk of loss, theft, damage or any unauthorised alterations.**	Management of the risk of loss, theft, damage, or unauthorised alterations
Liability of all trust service providers – assessment of financial risk	Recital (37): this regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this regulation should be applied in accordance with national rules on liability. Therefore, this regulation does not affect national rules on, for example, definition of damages, intention, negligence or relevant applicable procedural rules.	Insurance policies, set of limitations of liability in their terms of uses of the service
Security risk assessments and notification of security breaches	Recital (38): notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.	
	Article 8.2 (a): *assurance level low* shall refer to a means of electronic identification in the context of an electronic identification scheme, which	

	provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;
	Article 8.2 (b): *assurance level substantial* shall refer to a means of electronic identification in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;
	Article 12. 7: By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.
	Article 19: **Security requirements applicable to trust service providers** 1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.
	Article 24.2 C) on: **Requirements for qualified trust service providers** 2. A qualified trust service provider providing qualified trust services shall: (c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law.

TP-07-22-099-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

978-92-9204-569-2
10.2824/001991