ETSI TR 103 935 V1.1.1 (2023-12)

Cyber Security (CYBER);
Assessment of cyber risk based on products' properties to support market placement

Reference
DTR/CYBER-0094

Keywords
market placement, risk assessment

ETSI

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

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

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

Modal verbs terminology

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

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

Executive summary

Industry sectors have addressed the assessment of cyber risks, particularly as regards software, in a largely silo manner. On the other hand, recently introduced - and even upcoming - legislation mandates a horizontal treatment of cyber risks that spans multiple industry sectors and types of products. When it comes to cyber risks, for several these product families, these legislations are a first. And where such legislation holds for the placement of products and services in the EU Single Market, stringent requirements apply.

Given that risk assessment is predominantly informed by the context in which products and services operate, the (re)use of sectorial risk assessments (e.g. consumer, industrial, medical, etc.) in the development of technical standards supportive to such horizontal legislations has been a complex and arduous exercise. Particularly so when it comes to subjective factors - inherent in any risk assessment - that should be kept under control.

Currently, this is largely an open issue for the industry. Hence there is a need for an "adapter" concept (e.g. an approach, method, guidance, practice, or other suitable formalism) that facilitates reuse of the investment made by different industry sectors in the assessment of risk, while providing a uniform "interface" fit for the conformance assessment requirements and other legal concerns of such horizontal legislations. Such a unified "adapter" is currently lacking.

The present document addresses this gap and analyses the areas where subjective factors play a role in this context. It introduces the challenges that accompany the assessment of cyber risks in the context of market placement and presents essential principles that inform the risk assessment of products on the basis of their properties. Finally, a method to constrain and control subjectivity developed to address the challenges of said risk assessments is introduced and presented.

Introduction

Historically, risk assessment has been an exercise undertaken by a human expert in the domain. Thanks to the gradual accumulation of experience and knowledge about a particular domain, human experts have, in endless iteration, gone through the steps of the risk assessment process: risk identification, risk analysis, and risk evaluation.

However, even the most diligent application of expertise cannot preclude the possibility that different human experts, given the same information about risks, produce different assessment results. This is not due to an insufficient level of expertise, diligence, or some other aspect of professionalism, but rather an inherent characteristic that the involvement of a human actor begets.

Simply put, different people may assess the same piece of information differently.

Traditionally, cyber security has been a somewhat nice field in ICT. Cyber security experts have been - at least in comparison to other specialist areas in ICT - rare to find. The attainment of a competent level of expertise in cyber security requires a solid understanding of how all the ICT elements work together in any given scenario. As a result, competent cyber security experts are to commonly found in the mature stages of their professional life.

Simply because, acquiring expert knowledge of all the different technologies found in a modern globally distributed ICT system requires a considerable investment in one's career time. The continuous nature of technological evolution in ICT and the intelligent response of cyber adversaries means that cyber risks continuously evolve.

Cyber security experts and cyber adversaries are effectively in a continuous tug-of-war, where the latter seek to discover and exploit vulnerabilities in operational ICT systems and the former seek to shield those ICT systems against those vulnerabilities (as well as bring them back to an operational state if they fall victim to one).

In parallel, as ICT system pervade modern society ever more, concerns about safety, as well as other societal aspects of ICT systems and their elements gain more focus. These concerns include the impact of cyber risks.

Naturally, the legislative bodies of modern societies seek to address those concerns by the introduction of appropriate legislation. In the European Union, several strategic legislations have been introduced to addresses various concerns in connection to cyber risks. Among others, these include legislation that applies uniformly across all Member States of the European Union, such as the Delegated Regulation 2022/30 [i.19] that complements Directive 2014/53 [i.16], the proposal for a Cyber Resilience Act, and the proposal for an Artificial Intelligence Act.

However, when it comes to legislation that applies uniformly across all Member States of the European Union, stringent rules about the conformity assessment of products apply. These rules include the obligation assess all the risks that the (intended) use of a product and/or a service carries. This risk assessment informs the identification, evaluation, selection and application of risk treatments that reduce the overall risk exposure of the product and/or service to an acceptable level.

Standards play a role in this exercise by providing technical solutions - and the respective validation tests - to treat particular risks and declare conformity of a product and/or service on the basis of its compliance to those standards. These (harmonised) standards are developed by one or more European Standardization Organizations at the request of the European Commission, which ultimately reviews those harmonised standards. A critical aspect of that review concerns the application of validation tests that are objectively verifiable (i.e. that are reproducible).

A harmonised standard that passes the European Commission's review and gets a citation in the Official Journal of the European Union confers a presumption of conformity. The latter means that compliance to such a harmonised standard provides an indication that the respective product and/or service conforms to the legal requirements that the harmonised standard covers. And a declaration of conformity on the basis of compliance to such harmonised standards is as valid as an examination of the product and/or service by a third party. Hence when it comes to the placement of products and/or services in the EU Single Market, the self-declaration option offers the least economic friction to the placement of products and/or services in the EU Single Market.

And therein lies the conundrum: how can stakeholders assess risks in a way that (at least) converges to a common risk classification, so that the treatment of risks can be uniform across all stakeholders? To put it otherwise: for any given product and/or service, how can a risk assessment inform the treatment of cyber risks in a manner that does not diverge across stakeholders?

Lack of a common approach in the treatment of particular risks (which, in turn, depends on the risk assessment) means that option to self-declare a product's conformity is impossible for market stakeholders. In that case, the only option available is the examination of the product and/or service by a third-party and the consequent increase in the cost of market placement.

The present document addresses this conundrum. It proposes a method to enhance the presumption of conformity in cyber matters to a sufficient level.

1 Scope

The present document examines the background to the assessment of cybersecurity risks and identifies issues that may arise in the context of placing ICT products and services in the EU Single Market under the applicable legal requirements. Issues relevant to that scope are explored and options identified for possibly consideration in ETSI working practices to addresses these issues.

Under the New Legislative Framework (NLF) that governs the placement of products and services in the EU Single Market, harmonised standards provide a path of minimal economic friction for the agile introduction of technological innovations across EU Member States. In turn, risk assessment plays a pivotal role in the development of harmonised standards that, whilst supporting conformance to the applicable legal requirements, are also economically efficient.

The importance of harmonised standards to the smooth and efficient design and development of products and services to be placed on the EU Single Market has been recognized by the European Commission and the European Standardization Organizations.

Because the assessment of cyber risks is a fundamentally combinatorial exercise, the complexity and time it takes for a European Standardization Organization to identify and analyse the risk that should be considered in the harmonised standards increases exponentially with the scope that the respective legislation covers and the portfolio of ICT products and services it applies to. In simple terms, the greater the range of products and services within the scope of a particular legislation, the larger the set of possible use cases to consider will be, and thus the larger the workload of the risk assessment.

The present document presents the framework that underpins the placement of products in the EU Single Market in regard to risk assessment matters. It highlights of the salient features that, in accordance to common knowledge in the domain, good risk assessment approaches demonstrate. It also outlines the most common standards that underpin the application of risk assessment in an international context. In addition, it presents key characteristics of good approaches to the assessment of risks. Finally, it scopes the space of solutions that includes risk assessment approaches fit to inform the development and the application of harmonised standards in support of market placement.

The concepts and the approach put forth in the present document are applicable to products, as defined in [i.14], that are or can be described through properties that take distinct values.

The present document does not address the estimation of probability distributions that characterize the occurrence of events that contribute to particular risks. More specifically, it assumes that a stable body of knowledge in support of such estimates exists and builds on such estimates, if any, that apply in a given risk assessment scenario. A solution that, for illustration purposes, is shown in Annex A of the present document, assumes that errors in the estimation of numerical boundaries of risk classes follow a normal distribution. However, this assumption serves exclusively illustration purposes and does not restrict the application of the solution under the assumption of a different distribution.

Finally, in regard to the ICT industry's recent focus on zero trust [i.41] and vulnerability disclosure: zero trust is beyond the scope of risk assessment, as according to ISO 31000:2018 [i.2], enforcement actions are part of risk treatment, which, while informed by the outcomes of risk assessment, is beyond the scope of risk assessment. Likewise, vulnerability disclosure, whose ecosystem is presented in ETSI TR 104 003 [i.42], while informed by the outcomes of risk assessment, is beyond the scope of the risk assessment process itself.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

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

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

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

[i.1] ISO Guide 73:2009: "Risk management - Vocabulary".

[i.2] ISO 31000:2018: "Risk management - Guidelines".

[i.3] IEC 31010:2019: "Risk management - Risk assessment techniques".

[i.4] ISO 31073:2022: "Risk management - Vocabulary".

[i.5] ISO/IEC 27000:2018: "Information technology - Security techniques - Information security management systems - Overview and vocabulary".

[i.6] ISO/IEC 27002:2002: "Information security, cybersecurity and privacy protection - Information security controls".

[i.7] ISO/IEC 27005:2022: "Information security, cybersecurity and privacy protection - Guidance on managing information security risks".

[i.8] ISO/IEC TR 27016:2014: "Information technology - Security techniques - Information security management - Organizational economics".

[i.9] ISO/IEC 17000:2020: "Conformity assessment - Vocabulary and general principles".

[i.10] ISO/IEC 17060:2022: "Conformity assessment - Code of good practice".

[i.11] NIST SP 800-30 Revision 1: "Guide for Conducting Risk Assessments".

[i.12] "Cyber Threat Modelling: Survey, Assessment, and Representative Framework", MITRE Technical Paper, November 2018.

[i.13] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 laying down requirements for accreditation and market surveillance for the marketing of products and repealing Council Regulation (EEC) No 339/93.

[i.14] Decision No 768/2008/EC of the European Parliament and of the Council of 9 July 2008 on a common framework for the marketing of products, and repealing Council Decision 93/465/EEC.

[i.15] Regulation (EU) 2019/1020 of the European Parliament and of the Council of 20 June 2019 on market surveillance and compliance of products and amending Directive 2004/42/EC and Regulations (EC) No 765/2008 and (EU) No 305/2011.

[i.16] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC Text with EEA relevance.

[i.17] European Commission press release of October 29, 2021: "Commission strengthens cybersecurity of wireless devices and products".

[i.18] European Commission Q&A on Delegated Regulation 2022/30: "Strengthening cybersecurity of wireless devices and products".

[i.19] Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e) and (f), of that Directive.

[i.20] M/585 Commission Implementing Decision C(2022)5637 of 5.8.2022 on a standardisation request to the European Committee for Standardisation and the European Committee for Electrotechnical Standardisation as regards radio equipment in support of Directive 2014/53/EU of the European Parliament and of the Council and Commission Delegated Regulation (EU) 2022/30.

[i.21] The DoCRA Council: "Analysing Risk for Reasonable and Appropriate Safeguards".

[i.22] OpenGroup: "FAIR Requirements for Risk Assessment Methodologies".

[i.23] OpenGroup: "FAIR Risk Taxonomy (O-RT) V3.0.1".

[i.24] OpenGroup: "FAIR Risk Analysis Process Guide V1.1".

[i.25] OpenGroup: "FAIR The Mathematics of the Open FAIR Methodology".

[i.26] REDCA Technical Guidance Note 30: "Notified Body examination of a manufacturer's risk assessment under Annex III of Directive 2014/53/EU".

[i.27] European Commission: "Cyber Resilience Act - Fact Sheet".

[i.28] European Commission: "Proposal for a Regulation laying down harmonised rules on artificial intelligence".

[i.29] European Commission: "Impact Assessment of the Regulation on Artificial intelligence".

[i.30] European Commission: "The EU Cybersecurity Act".

[i.31] European Commission: "Implementing Decision (EU) 2019/417, Guidelines for the management of the European Union Rapid Information System 'RAPEX'".

[i.32] European Commission: "EU general risk assessment methodology", Action 5 of Multi-Annual Action Plan for the surveillance of products in the EU (COM(2013)76), Ref. Ares(2016)2656912.

[i.33] European Commission: "The 'Blue Guide' on the implementation of EU product rules 2022".

[i.34] "EU Cybersecurity Certification".

[i.35] ISO/IEC 15408-1:2022: "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.36] ISO/IEC 15408-2:2022: "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 2: Security functional components".

[i.37] ISO/IEC 15408-3:2022: "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components".

[i.38] Recommendation ITU-T X.1055: "Risk management and risk profile guidelines for telecommunication organizations".

[i.39] Recommendation ITU-T X.1208: "A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies".

[i.40] NIST SP 800-154: "Guide to Data-Centric System Threat Modelling".

[i.41] NIST SP-800-207: "Zero trust architecture".

[i.42] ETSI TR 104 003: "Cyber Security (CYBER); The vulnerability disclosure ecosystem".

[i.43] ISO/IEC 27001:2022: "Information security, cybersecurity and privacy protection Information security management systems".

[i.44] ETSI EN 302 217-2: "Fixed Radio Systems; Characteristics and requirements for point-to-point equipment and antennas; Part 2: Digital systems operating in frequency bands from 1 GHz to 86 GHz; Harmonised Standard for access to radio spectrum".

[i.45] IEEE 802.15.1-2005: "IEEE™ Standard for Information technology - Local and metropolitan area networks - Specific requirements - Part 15.1a: Wireless Medium Access Control (MAC) and Physical Layer (PHY) specifications for Wireless Personal Area Networks (WPAN)".

[i.46] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ISO Guide 73:2009 [i.1] and the following apply:

action: act taken against an Asset by a Threat Agent

NOTE: Requires first that contact occurs between the Asset and Threat Agent [i.23].

asset: anything that has value to the organization

NOTE 1: As defined in ISO/IEC 27002:2002 [i.6].

NOTE 2: The information, information system, or information system component that is breached or impaired by the Threat Agent in a manner whereby its value is diminished or the act introduces liability to the Primary Stakeholder [i.23].

conformity assessment: demonstration that specified requirements are fulfilled

NOTE: As defined in ISO/IEC 17060:2022 [i.10].

consequence: outcome of an event affecting objectives

NOTE: As defined in ISO Guide 73:2009 [i.1].

contact event: occurs when a Threat Agent establishes a physical or virtual (e.g. network) connection to an Asset

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

contact frequency: probable frequency, within a given timeframe, that a Threat Agent will come into contact with an Asset

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

control: measure that maintains and/or modifies risk

NOTE 1: As defined in ISO 31000:2018 [i.2].

NOTE 2: Any person, policy, process, or technology that has the potential to reduce the Loss Event Frequency (LEF) - Loss Prevention Controls - and/or Loss Magnitude (LM) - Loss Mitigation Controls [i.23].

equivalence: sufficiency of different conformity assessment results to provide the same level of assurance of conformity with regard to the same specified requirements

NOTE: As defined in ISO/IEC 17000:2020 [i.9].

event: occurrence or change of a particular set of circumstances

exposure:

- extent to which an organization and/or stakeholder is subject to an event

NOTE 1: As defined in ISO Guide 73:2009 [i.1].

- extent to which an organization and/or interested party is subject to an event

NOTE 2: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

level of risk: magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

likelihood: chance of something happening

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

loss: reduction in the value of an asset

NOTE: As defined in ISO/IEC TR 27016:2014 [i.8].

loss event: occurs when a Threat Agent's action (Threat Event) is successful in breaching or impairing an Asset

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

loss event frequency: probable frequency, within a given timeframe, that a Threat Agent will inflict harm upon an Asset

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

loss flow: structured decomposition of how losses materialize when a Loss Event occurs

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

loss magnitude: probable magnitude of loss resulting from a Loss Event

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

loss scenario: story of loss that forms a sentence from the perspective of the Primary Stakeholder

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

market availability: act of making a product available in the EU Single Market

NOTE: A product is made available on the market when supplied for distribution, consumption or use on the Union market in the course of a commercial activity, whether in return for payment or free of charge [i.33].

market placement: act of placing a product in the EU Single Market

NOTE: A product is placed on the market when it is made available for the first time on the Union market. According to Union harmonization legislation, each individual product can only be placed once on the Union market [i.33].

primary stakeholder: person or organization that owns or is accountable for an Asset

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

probability: measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

probability of action: probability that a Threat Agent will act against an Asset once contact occurs

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

residual risk: remaining risk after risk treatment

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

resilience: adaptive capacity of an organization in a complex and changing environment

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

risk: effect of uncertainty on objectives

NOTE 1: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

NOTE 2: The probable frequency and probable magnitude of future loss [i.23].

risk analysis: process to comprehend the nature of risk and determine the level of risk

NOTE: As defined in ISO Guide 73:2009 [i.1], ISO 31073:2022 [i.4] and FAIR Risk Taxonomy (O-RT) [i.23].

risk assessment: overall process of risk identification, risk analysis, and risk evaluation

NOTE: As defined in ISO Guide 73:2009 [i.1], ISO 31073:2022 [i.4] and FAIR Risk Taxonomy (O-RT) [i.23].

risk control: measure that maintains and/or modifies risk

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

risk criteria: terms of reference against which the significance of a risk is evaluated

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

risk evaluation:

- process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable

NOTE 1: As defined in ISO Guide 73:2009 [i.1].

- process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable or tolerable

NOTE 2: As defined in ISO 31073:2022 [i.4].

risk factors: individual components that determine risk, including Loss Event Frequency, Loss Magnitude, Threat Event Frequency, etc.

NOTE: As defined in FAIR Risk Taxonomy (O-RT) [i.23].

risk identification: process of finding, recognizing and describing risks

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

risk management: coordinated activities to direct and control an organization with regard to risk

NOTE: As defined in ISO Guide 73:2009 [i.1], ISO 31073:2022 [i.4] and FAIR Risk Taxonomy (O-RT) [i.23].

risk source: element which alone or in combination has the potential to give rise to risk

NOTE: As defined in ISO Guide 73:2009 [i.1] and ISO 31073:2022 [i.4].

risk tolerance:

- organization's or stakeholder's readiness to bear the risk after risks treatment in order to achieve its objectives

NOTE 1: As defined in ISO Guide 73:2009 [i.1].

- organization's or interested party's readiness to bear the residual risk in order to achieve its objectives

NOTE 2: As defined in ISO 31073:2022 [i.4].

risk treatment: process to modify risk that can involve:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk.