# 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

# 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.

- Taking or increasing risk in order to pursue an opportunity.
- Removing the risk source.
- Changing the likelihood.
- Changing the consequences.
- Sharing the risk with another party or parties (including contracts and risk financing).
- Retaining the risk by informed decision.

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

**secondary stakeholder:** individuals or organizations that may be affected by events that occur to Assets outside of their control

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

EXAMPLE: Consumers are Secondary Stakeholders in a scenario where their personal private information may be inappropriately disclosed or stolen.

**threat:**

- potential cause of an unwanted incident, which can result in harm to a system or organization

NOTE 1: As defined in ISO/IEC 27000:2018 [i.5].

- potential source of danger, harm, or other undesirable outcome

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

NOTE 3: Anything that is capable of acting in a manner resulting in harm to an Asset and/or organization [i.23]. For example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.

**threat agent:** any agent (e.g. object, substance, human) that is capable of acting against an Asset in a manner that can result in harm

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

**threat capability:** probable level of force (as embodied by the time, resources, and technological capability) that a Threat Agent is capable of applying against an Asset

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

**threat community:** subset of the overall Threat Agent population that shares key characteristics

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

**threat event:** occurs when a Threat Agent acts against an Asset

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

**threat event frequency:** probable frequency, within a given timeframe, that a Threat Agent will act against an Asset

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

**vulnerability:** intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence

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

NOTE 2: The probability that a Threat Event will become a Loss Event; probability that Threat Capability is greater than Resistance Strength. (Synonym: Susceptibility) [i.23].

**zero trust:** cybersecurity paradigm "to enforce" accurate, least privilege per-request access decisions in information systems and services

## 3.2 Symbols

Void.

## 3.3 Abbreviations

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

| | |
|---|---|
| AI | Artificial Intelligence |
| ATT&CK | Adversarial Tactics, Techniques and Common Knowledge |
| CEN | European Committee for Standardization |
| CENELEC | European Committee for Electrotechnical Standardization |
| CRA | Cyber Resilience Act |
| CSA | Cyber Security Act |
| CSP | Constrain Satisfaction Problem |
| CSPRNG | Cryptographically Secure PseudoRandom Number Generator |
| DDoS | Distributed Denial of Service |
| DoC | Declaration of Conformity |
| DoCRA | Duty of Care Risk Analysis |
| DREAD | Damage, Reproducability, Exploitability, Affected users, Discoverability |
| EC | European Commission |
| ENISA | European Union Agency for Cybersecurity |
| ESO | European Standardization Organization |
| ETSI | European Telecommunications Standards Institute |
| EU | European Union |
| GPSD | General Product Safety Directive |
| hEN | harmonised European Norm |
| ICT | Information and Communication Technologies |
| IEC | International Electrotechnical Commission |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| ITU | International Telecommunications Union |
| JTB | Joint Technical Body |
| LEF | Loss Event Frequency |
| LM | Loss Magnitude |
| NIST | National Institute of Standards and Technology |
| NLF | New Legislative Framework |
| OJEU | Official Journal of the European Union |
| PBRA | Property-Based Risk Assessment |
| PII | Personally Identifiable Information |
| RAPEX | Rapid Exchange of Information System |
| RDF | Resource Description Framework |
| RED | Radio Equipment Directive |
| SOHO | Small Office Home Office |
| SQL | Structured Query Language |
| STRIDE | Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privilege |
| TOE | Target Of Evaluation |
| TRNG | True Random Number Generator |
| TVRA | Threat Vulnerability and Risk Analysis |

# 4 Market placement in the EU Single Market

## 4.1 Introduction

The term EU Single Market refers to the internal market of the European Union (EU). The latter is a single market in which the free movement of goods, services, capital and persons is assured. In order for a product to be legally sold in the EU Single Market, it has to successfully undergo market placement in accordance to the procedures set forth by the New Legislative Framework (NLF) [i.13], [i.14] and [i.15].

The most comprehensive guide to the placement of products in the EU Single Market under the NLF is the Blue Guide [i.33] that:

a) lays out the general principles of product legislation in support of consumer protection in the EU, and

b) contributes to a coherent application of these rules.

The Blue Guide was revised and published in June 2022 to reflect recent changes in the legislation, particularly in regard to the adoption of the Regulation on Market Surveillance Regulation (EU) 2019/1020 [i.15]. The latest version addresses particular concerns identified through the experience in the application of the New Legislative Framework (NLF) in the case of ICT products, as well as developments in the membership of the EU Single Market:

a) It provides examples of the term "own use exemptions" in market placement.

b) It reflects the objective of the European Commission for the right to repair.

c) It acknowledges the impact of cybersecurity on risk and addresses the modification of software post market placement through the classification of software updates as similar to physical repairs and modifications.

d) It clarifies the need for the continuous update of the Declaration of Conformity (DoC).

e) It elaborates on the role and obligations of fulfilment service providers and the obligations that Regulation (EU) 2019/1020 [i.15] attaches to online sales.

f) It addresses the withdrawal of the United Kingdom from the EU and the status of Northern Ireland.

The Blue Guide addresses market placement matters and serves as reference guidance for economic stakeholders that wish to market products and/or services in a harmonized way across the European Union [i.33].

## 4.2 Conformance under the New Legislative Framework (NLF)

### 4.2.1 General

In regard to the assessment of a product's conformance to the legislations applicable, two options are available under the NLF and the Blue Guide [i.33]:

a) Declaration of Conformity (DoC) - Module A - that can be on the basis of any combination of:

   1) Harmonised standards

   2) Common specifications (where so prescribed by the respective legislation)

   3) Other instruments (where so prescribed by the respective legislation)

b) EU type examination (involvement of Notified Bodies) - Modules B to Module H.

### 4.2.2 Option 1 - Declaration of Conformance (DoC)

The presumption of conformity under the NLF is based on the confidence that comes with the physically measurable results that the respective tests yield. In particular, conformity assessment is informed exclusively by properties of the subject and by measurements of those properties. Historically, these measurements have taken place under the laws of physics.

Under the NLF, for any given product, harmonized standards apply equally to all economic stakeholders that place the said product in the EU Single Market. This requires that, as far as the information about the product that the harmonised standards and the test they contain refer to is concerned, the product does not differ across these economic stakeholders.

In turn, this requires that, for any given product, the application of the harmonised standards and the tests they contain against the information about that product should yield reproducible results that reflect its performance. In other words, the application of harmonised standards to identical products, insofar the information about these products that the harmonised standards and the test they contain refer to is concerned, should yield identical results.

Because the application of harmonised standards is expected to support legal certainty, the manner in which the results of tests contained in the harmonised standards may be interpreted for purposes of conformity assessment under the NLF is restricted to "Yes" or "No" (i.e. deterministic binary) outcomes. This is necessary because it is not acceptable that the application any ambiguity about a product's conformance exists.

A key aspect of conformity assessment under the NLF concerns the accuracy of measurement. In order to support presumption of conformity to the essential requirements of market placement, a harmonized standard should provide confidence in the assessment of conformity of the products in its scope. That confidence is established through norms in regard to the accuracy of measurement for the product's properties that the harmonised standard refers to.

In the cybersecurity domain, threat modelling and risk assessment deal with unknowns. This is because it is impossible to fully observe, understand, know, or anticipate adversaries and their behaviours. Neither is it possible to enumerate all potential vulnerabilities in a given system. Even if, at a particular time instance, complete knowledge about threats and adversaries was available, confidence in it would degrade over time, as adversaries constantly adapt their tactics. As a result, threat models and risk assessments are, inevitably, estimations of reality that one formulates given a sample of reality.

The key difference between accuracy and estimation is that the former is governed by the technological limitations of measurement instruments, which, in turn, are governed by the laws of physics, while the latter is governed by the subjective nature that comes with the cognitive processes of human beings. Cybersecurity is thus not a matter of absolutes, but rather a discipline of good practice that evolves as threats and risks evolve.

For a harmonised standard (that is cited in the Official Journal of the European Union) to support presumption of conformity with regard to a cybersecurity concern, it should either include or refer to norms that provide confidence in the estimation of threats and risks. Given the level of desirable confidence, these norms can provide guidance in regard to the treatment of subjective factors that entail threat modelling and risk assessment.

Such norms may also be based on scientific approaches that deal with uncertainty (e.g. fuzzy logic, etc.). Having a scientifically grounded approach means that the outcomes these norms would yield can be bound to a performance envelope and, thus, support the assertions necessary in conformance assessment.

EXAMPLE: A common characterization of product considers its capabilities to classify it in a so-called constrained category. This is even more common in the Internet of Things sector where product may come in a highly embedded form and be subject to power budget limitations.

### 4.2.3 Option 2 - EU type examination (involvement of Notified Bodies)

When a harmonised standard is not used in full (see Figure 1 in [i.32]), a manufacturer cannot benefit of the presumption of conformity therefore an EU type examination is necessary before to put a product on the market. For instance, when a harmonised standard is not cited in the OJEU, notified bodies carry out the tasks pertaining to the conformity assessment procedures referred to in the applicable technical harmonization legislation [i.33].

A conformity assessment body is a body that performs one or several elements of conformity assessment, including one or several of the following activities: calibration, testing, certification and inspection. Notified bodies are conformity assessment bodies which have been officially designated and notified by their national authority to carry out the procedures for conformity assessment within the meaning of applicable Union harmonization legislation when a third party is required. They are called "notified bodies" under EU legislation [i.33].

## 4.3 On the risk of products

In the New Legislative Framework (NLF), the economic stakeholder that places a product in the EU Single Market (i.e. typically the manufacturer of the final product) addresses product safety. The economic stakeholder is responsible for the assessment of all kinds of risks that the use (and the reasonable foreseeable misuse) of the product carries.

Hence the scope of the risk assessment undertaken by the economic stakeholder is responsible for including all kinds of mechanical, chemical, electrical and risks relevant to the software elements of the product. The scope of this initial risk assessment undertaken by the economic stakeholder includes also software and the respective cyber risks (e.g. risks due to the loss of connectivity) [i.33].

Software may be subject to updates throughout its lifetime, some of which may substantially modify the software and/or its functions. The Blue Guide defines the criteria for when a software update classifies as a substantial modification:

a) The software update modifies the original intended functions, type or performance of the product and this was not foreseen in the initial risk assessment.

b) The nature of the hazard has changed or the level of risk has increased because of the software update.

c) The product is made available (or put into service where this is covered by the specific Union harmonization legislation).

In the context of their obligation to assess the risks of the product, and where harmonised standards in support of the legislation whose scope includes the product are cited in the OJEU, economic stakeholders may inform their risk assessment activities by the information about risk in the said harmonised standards, if any.

That such harmonised standards include information about the risks of the product does not waive the obligation of the economic stakeholder to conduct a risk assessment.

This is necessary even if the economic stakeholder applies harmonised standards (whose reference is published in the OJEU and which aims to cover certain risks) to satisfy essential requirements of the applicable legislation, as it does not automatically follow that the said harmonised standards cover all the risks of the product.

It is not a given that the harmonised standards, where available, cover all essential requirements of all legislative acts applicable to a given product, nor that they cover all essential requirements of a specific legislation. Even if that was the case, the product in question (in the context of its intended use) may introduce additional risks not considered in the harmonised standards. However, the manufacturer should still consider those additional risks in their risk assessment.

Hence the assessment of the risks of the product remains a mandatory activity of the economic stakeholder that places a product on the EU Single Market.

# 5 Legislative landscape

## 5.1 Introduction

This clause lists the major legislative acts in the European Union that, directly or indirectly, or requires a risk assessment in the context of cyber issues.

It is noted that these legislative acts are not by definition mutually exclusive as regards their scope of applicability (i.e. for any given product, service or process, multiple legislative acts may apply simultaneously).

## 5.2 Cyber Security Act (CSA)

Cited in the Official Journal of the European Union on June 7, 2019, the European Cybersecurity Act [i.30] aims to achieve a high level of cyber security, cyber resilience and trust in the European Union (EU). It does so by:

- Setting objectives, tasks and organizational matters for a strengthened and renamed European Union Agency for Cybersecurity (ENISA), with a new permanent mandate. In particular, ENISA is mandated to:
  - Increase operational cooperation at EU level.
  - Help EU Member States who wish to request it to handle their cybersecurity incidents.
  - Support the coordination of the EU in case of large-scale cross-border cyberattacks and crises.
- Establishing a framework for voluntary European cybersecurity certification schemes for Information and Communications Technology (ICT) products, services and processes.

The certification framework will provide certification schemes [i.34] that area applicable across the EU as a comprehensive set of rules, technical requirements, standards and procedures. The framework relies on agreement at EU level on the evaluation of the security properties of a specific ICT product, service or process.

The framework that CSA introduces provides the building blocks to develop certifications schemes that, in turn, can attest that ICT products and services that have been certified in accordance with particular CSA scheme comply with the requirements addressed by the respective scheme.

In particular, each European scheme specifies:

- The categories of products and services covered.
- The cybersecurity requirements, such as standards or technical specifications.
- The type of evaluation (e.g. self-assessment or third party).
- The intended level of assurance.

The CSA framework defines three (3) levels of assurance:

- Basic
- Substantial
- High

The levels of assurance are commensurate with the level of risk associated with the intended use of the product, service or process, in terms of probability and impact of an accident.

## 5.3 Radio Equipment Directive (RED) Delegated Regulation

On June 24, 2022, the Commission published in the Official Journal of the EU the Commission Delegated Regulation (EU) 2022/30 [i.19] adopted by the Commission on 17 March 2022 and endorsed by the co-legislators following a scrutiny procedure that ended on 17 June 2022 [i.18].

According to the respective press release, Delegated Regulation 2022/30 [i.19] is designed to improve the cyber security of product (i.e. radio equipment in the scope and terminology of Directive 2014/53/EU [i.16] as follows:

a) Improve network resilience

   Wireless products (i.e. radio equipment) will have to incorporate features to avoid harming communication networks and prevent the possibility that the devices are used to disrupt website or other services functionality [i.18].

b) Better protect consumers' privacy

   Wireless devices and products will need to have features to guarantee the protection of personal data. The protection of children's rights will become an essential element of this legislation. For instance, manufacturers will have to implement new measures to prevent unauthorized access or transmission of personal data [i.18].

c) Reduce the risk of monetary fraud

   Wireless devices and products will have to include features to minimize the risk of fraud when making electronic payments. For example, they will need to ensure better authentication control of the user in order to avoid fraudulent payments [i.18].

Delegated Regulation 2022/30 [i.19] activates the (so far inactive) Articles 3(3) (d, e, f) of Directive 2014/53/EU [i.16] and defines the categories of product (i.e. radio equipment in the scope and terminology of Directive 2014/53/EU [i.16]) that are in their scope as follows:

a) Devices capable of communicating over the Internet

   Examples of such equipment include electronic devices such as smartphones, tablets, electronic cameras; telecommunication equipment as well as equipment that constitutes the "internet of things". Due to insufficient security, such devices present a risk that third parties can improperly access and share personal data, including for fraud purposes, or that such equipment is misused to harm the network [i.19].

b) Toys and childcare equipment

   Toys and baby monitors can be vulnerable to cybersecurity threats that monitor or collect information about children. Therefore, the protection of children's rights constitutes an essential element of this legislation [i.19].

c) Wearables

   Devices like smartwatches and fitness trackers are more and more present in our lives and they collect biometric data [i.19].

On August 5, 2022, the European Commission issued a standardization request to CEN and CENELEC to develop harmonised standards in support of Delegated Regulation 2022/30.

## 5.4 Artificial Intelligence Act (AI Act)

On April 21, 2021, the European Commission published a proposal for a regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence and amending certain union legislative acts [i.28]. Henceforth known as the Artificial Intelligence Act (AI Act) [i.28], this proposal sets specific objectives:

- To ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values.
- To ensure legal certainty to facilitate investment and innovation in AI.
- To enhance governance and effective enforcement of existing law on fundamental rights and safety requirements applicable to AI systems.
- To facilitate the development of a single market for lawful, safe and trustworthy AI applications and prevent market fragmentation.

The AI Act [i.28] sets harmonized rules for the development, placement on the market and use of AI systems in the EU Single Market on the basis of a proportionate risk-based approach. Thus the AI Act fills key gaps in EU law:

- A definition of an AI system.
- Horizontal rules related to the classification of risks related to AI technologies.

In addition, the AI Act [i.29]:

- Sets risk assessment methodology and defines high-risk AI systems.
- Sets certain minimum requirements for high risk AI systems (e.g. minimum transparency of algorithm, documentation, data quality).
- Sets legal obligations with regard to the conduct of key economic operators (providers and users).
- Sets a governance system at national and EU level for the effective enforcement of these rules.

In the AI Act the classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used [i.29].

More specifically, Title III of the AI Act [i.28] sets the classification rules and identifies two main categories of high-risk AI systems:

- AI systems intended to be used as safety component of products that are subject to third party ex-ante conformity assessment.
- Other standalone AI systems with mainly fundamental rights implications that are explicitly listed in Annex III of the AI Act.

## 5.5 Cyber Resilience Act (CRA)

On September 15, 2022, the European Commission published a proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements that amends Regulation (EU) 2019/1020 [i.27]. Henceforth known as the Cyber Resilience Act (CRA) [i.27], this proposal sets specific objectives:

- To ensure that products with digital elements placed on the EU market have fewer vulnerabilities and that manufacturers remain responsible for cybersecurity throughout a product's life cycle.
- To improve transparency on security of hardware and software products.
- To benefit business users and consumers through better protection.

To achieve its objectives the CRA [i.27] stipulates additional requirements for economic operators (manufacturers):

- That cybersecurity is considered throughout the product's lifecycle (i.e. in planning, design, development, production, delivery and maintenance phases).
- That all cybersecurity risks are documented.
- Manufacturers will have to report actively exploited vulnerabilities and incidents.
- Once sold, manufacturers are responsible for ensuring that for the expected product lifetime or for a period of five years (whichever is the shorter), vulnerabilities are handled effectively.
- That clear and understandable instructions for the use of products with digital elements are available.
- That security updates are made available for at least five years.

The CRA introduces harmonized rules for the placing on the market of connected hardware and software products. It does so by means of essential cybersecurity requirements for the design and development of products with digital elements as well as obligations for all economic operators in the value chain. These harmonized rules define the duty of care for the whole life cycle of products with digital elements [i.27].

## 5.6 Conclusion

Each of these regulations (that are already in force or in preparation) requires a risk assessment in the context of cyber issues. However, none of these legislations describes in detail how a risk assessment should be done.

The present document presents general methodologies for risk assessment and proposes a particular approach to the assessment of risks.

# 6 Overall concept of risk assessment process

## 6.1 Introduction

In accordance to NLF and the Blue Guide an economic stakeholder that places a product or service in the EU Single Market is responsible for carrying out a risk assessment. The latter should be sufficiently documented, by the economic stakeholder, as part of the market placement documentation. Hence the risk assessment is an obligation of the economic stakeholder that places a product in the EU Single Market (i.e. under the NLF).

In fact, irrespective of the legal requirement, it is recommended that the manufacturer caries out a risk assessment for their product before considering what actions are required.

The discussion thus far makes it abundantly clear that current and upcoming legislation in the area of cybersecurity and privacy requires a risk assessment. However, no approach that can achieve a consistent assessment of risk by different stakeholders (without any additional assumptions about those stakeholders) yet exists.

This clause explores the perspectives of the different stakeholders in the NLF in regard to risk assessment matters.

## 6.2 Principles

As a general principle, under the NLF, any approach that will guide risk assessment in the context of market placement under the NLF should not restrict the conformity assessment options available to an economic stakeholder (e.g. between 1st party, 2nd party and 3rd party assessment, where applicable).

Conformity assessment under the NLF is informed exclusively by the declaration of intended use by the economic stakeholder. Hence, as a general principle, the application of the risk and/or threat methodology is informed exclusively by the declaration of intended use provided in connection to the product's placement in the EU market.

Furthermore, the treatment of threat modelling and risk assessment is scoped exclusively to the information that is part of the definition of the intended use of product in regard to market placement under the NLF. Additional information that is not part of the definition of the intended use of the product in regard to market placement under the NLF, is out of scope.

## 6.3 Working assumptions

For the rest of the present document, the definition of the intended use of the product is understood, as a minimum, to include the following information:

a) The environment in which the product should nominally operate.

b) The nature of the data to protect that is under control of the product.

The definition of the intended use of the product may, at the discretion of the economic stakeholder, include additional information. The present document does not consider any assumptions as to what that additional information may be.

## 6.4 Stakeholder perspectives

### 6.4.1 Introduction

In regard to the conformity of a products placed in the EU Single Market, the key stakeholders include:

1) the European Standardization Organizations;

2) the Economic Stakeholder (i.e. the entities that place products in the EU Single Market);

3) the Notified Bodies (i.e. the entities that undertake an EU-type examination activity); and

4) the Market Surveillance authorities.

### 6.4.2 European Standardization Organization (ESO)

Where a European Standardization Organization accepts a Standardization Request and undertakes the development of harmonised standards in support of the essential requirements of legislation that addresses cyber aspects, it is common that the need for a risk assessment arises.

This risk assessment serves the need to identify technical requirements that are applicable and/or appropriate for the essential requirements they should cover and be proportionate to the level of risk. Historically the types of risk would include primarily risks of physical harm to an individual - typically the user of the product in question.

However, [i.20] that requests the development of harmonised standards for Delegated Regulation 2022/30 [i.19] requires that the "*harmonised standards shall be drafted and revised by applying the iterative process of risk assessment and risk reduction*". This clearly requires that the European Standardization Organization that accept [i.20], as part of their development process, conduct a risk assessment.

In [i.20] the requirement to conduct a risk assessment is part of the specific requirements for these harmonised standards. The specific requirements applicable to a harmonised standard are part of the information that the review of the harmonised standard considers in order to determine whether the harmonised standard is suitable for citation in the Official Journal of the European Union.

Thus it is important that the risk assessment that an ESO would undertake in response to [i.20] is not only properly designed, formulated and instrumented, but also documented as part of the standardization deliverables in support of the harmonised standards.

### 6.4.3 Economic Stakeholder

In the NLF the economic stakeholder (e.g. manufacturer, distributor, etc.) that places a product in the EU Single Market addresses product safety. The economic stakeholder is responsible for the assessment of all kinds of risks that the use (and the reasonable foreseeable misuse) of the product carries.

Under the NLF essential requirements apply as a function of the hazard inherent to a given product. The Blue Guide on the Implementation of EU Product Rules 2022 [i.33] clearly requires that "*manufacturers have to carry out a risk analysis to first identify all possible risks that the product may pose and determine the essential requirements relevant for the product*". This analysis implies that the economic stakeholder (manufacturer) should:

- Assess all the different elements of the products and determine which harmonization legislation applies to it, and which specific essential requirements as set out therein.
- Document this analysis and include it in the technical documentation.
- Document the assessment of how the risks identified are addressed to ensure that the product complies with the relevant essential requirements (for example, by applying harmonised standards). If only part of the harmonised standard is applied or it does not cover all relevant essential requirements, then the way relevant essential requirements not covered by it are dealt with, should be documented.

As an example, under the Radio Equipment Directive (RED) 2014/53/EU [i.16], [i.26] stipulates that the risk analysis done by the economic stakeholder (e.g. manufacturer, distributor, etc.) and assessed by the notified body follows the guidance given in Blue Guide 2022 under clause 4.3 and clause 4.1.2.2. Hence the risk analysis and assessment should consider and document at least the following steps:

1) Clearly identifying the intended user groups (e.g. professional, consumer, children, etc.) and the operating environment (e.g. Indoor/outdoor, temperature, altitude, etc.) for which the product is intended to be used.
2) Identifying which of the essential requirements of the directive are applicable. The essential requirements of Articles 3.1 and 3.2 apply to all radio equipment, whereas the essential requirements of each paragraph of Article 3.3 only apply to the radio equipment within scope of that paragraph.
3) Identifying which harmonised standard(s) or equivalent documentation has been applied to mitigate the risk of non-compliance to the Essential Requirements.
4) Specifically identifying if there are special product characteristics or features which might not be included in the current harmonised standard(s) and how these features are still considered to comply with the essential requirements (i.e. the requirements set in the legislative acts that form the respective harmonization legislation).

The manufacturer should carefully check the legislation he wishes to demonstrate compliance to, in order to ensure that their equipment does come under that legislation and that there are no exemptions (i.e. medical devices are exempt from Delegated Regulation 2022/30).

### 6.4.4 Notified Body

The Notified Body stakeholder is an essential aspect of the NLF that arguably complements harmonised standards in the matters of conformance assurance that the placement of products and/or services in the EU Single Market entails.

For instance, under the Radio Equipment Directive (RED) 2014/53/EU [i.16], Annex III, Part A, Module B 3(c), it is required that a notified body assesses the technical documentation associated with the apparatus (i.e. the radio equipment) to ensure conformity with the essential requirements set out in Article 3 of the Radio Equipment Directive (RED) 2014/53/EU [i.16] and that the technical documentation includes an adequate analysis and assessment of the risk(s) [i.26].

Under the RED, risk assessment is an activity for the manufacturer to perform. However, a notified body takes the manufacturer's risk assessment into account as provided in the manufacturer's technical documentation when performing an EU-Type examination assessment under Annex III of the RED [i.26]. To that end, [i.26] stipulates that:

1) The notified body checks that the manufacturer's technical documentation for the radio equipment contains a risk assessment analysis.

2) The notified body checks whether the risk analysis is compliant with the minimum requirements in the Blue Guide and take into consideration the content of this guide.

3) The notified body checks whether the risk analysis is adequate for the radio equipment under review, with regard to section 2 of [i.26].

4) The notified body considers for their assessment the information presented in the risk analysis and assessment by the manufacturer.

5) The notified body allows any format and structure of the risk analysis and assessment as part of the technical documentation because this is entirely determined by the manufacturer.

6) The notified body considers whether the manufacturer's defined user groups and operational conditions are appropriate. For example, if the product is intended to be used by vulnerable people, or if the product is intended to be used in conditions outside of the scope of the applied harmonised standards, etc.

7) The notified body assesses whether the harmonised standards, other normative documents, and reference documents applied by the manufacturer entirely cover the essential requirements for which they have been selected.

8) If the product is covered by more than the RED, such as a radio equipment incorporated into a device subject to the Medical Equipment Regulation, then a more onerous risk assessment may be required by the other directive. The RED notified body should take care not to exceed their remit under the RED.

9) The notified body take cares that any exceptional product characteristics identified are considered in the risk assessment which might not have been dealt with or known at the time the applied harmonised standard(s) had been prepared. It can be expected that this may only occur in very rare, exceptional cases.

10) Annex V d) of the RED requires that where harmonised standards are not applied, a description is required of the solutions adopted to meet the essential requirements of Article 3. This requirement applies to cases where the harmonised standard exists but was not fully applied, or when the appropriate standard is not harmonised in the RED Official Journal of harmonised standards (OJEU). It applies to all parts of Article 3.1a, 3.1b, 3.2 and 3.3 of the RED. The description of the required solutions and the manufacturer's decision for choice of solution should be detailed in the risk assessment.

While [i.26] details the steps above, several key terms lack a definition that is common between all notified bodies - let alone between all economic stakeholders and all notified bodies. In other words, these steps may be interpreted differently by different actors and yield different results.

Perhaps an approach that relies on an implicit interpretation of terms can be sufficiently stable (i.e. lead to the same interpretation by different actors) in a setting where stable norms prevail (e.g. where the risks at hand are governed by the laws of physics for which a wide consensus long exists).

However, it seems unlikely that an implicit interpretation of terms offers sufficient stability (i.e. not lead to different interpretations) in cyber matters where one operates under incomplete information and assumptions about third parties and other largely unknown factors (and their rate of change) are unavoidable.

### 6.4.5 Market Surveillance Authority

On October 16, 2015, as part of the Multi-Annual Action Plan for the surveillance of products in the EU, the European Commission issued guidance in the form of an EU general risk assessment methodology [i.32].

This EU general risk assessment methodology implements Article 20 of Regulation (EC) No 765/2008 and is intended to assist market surveillance authorities when they assess the compliance of products that are subject to Union harmonization legislation (i.e. products in the EU Single Market) [i.32].

The methodology builds on the RAPEX Guidelines [i.31], developed within the framework of the Directive on General Product Safety (GPSD) and extends them in two respects:

- To make sure that the broader categories of public risk protected under EU harmonization legislation can be considered.
- To reflect the specific legal requirements on harmonized products.

The objective of the methodology [i.32] is to provide guidance to authorities on the aspects below:

- When rapid intervention is needed.
- Whether a RAPEX notification should be made.
- Which measures to take in relation to the non-conformity of a product (proportionality).

The guidance notes that the risk assessment of a harmonized product does not replace the evaluation of the compliance of the product with the requirements laid down in EU legislation and the relevant harmonised standards. In fact, the risk assessment of a harmonized product complements the product compliance evaluation, as it allows the assessment of the seriousness of the possible consequences of non-compliance [i.32]. Hence the risk assessment of a harmonized product is inherently linked to the evaluation of its compliance with legal requirements.

Notably, the guidance suggests that market surveillance authorities, in identifying and assessing the hazards associated to a product, should, as much as possible, use the information that has been made available by the economic stakeholder (manufacturer) as part of the product's placement in the EU Single Market:

- The Declaration of Conformance
- The Technical Documentation

Because compliance to the essential requirements, as a function of the hazard inherent to the product, is expected under market placement, economic stakeholders are responsible for conducting a risk analysis and determining the essential requirements applicable to the product in question. This risk analysis is part of the technical documentation, unless risk assessment is covered by the respective harmonised standards [i.32].

The methodology builds on the RAPEX Guidelines to determine the potential harm (that results through an injury) to the consumer [i.32]. However, as the scope of the RAPEX Guidelines does not extend beyond consumer products, the methodology is not applicable in scenarios that are not purely consumer ones).

This should not come as a surprise. The purpose of the RAPEX Guidelines is to provide, within the framework of the Directive on General Product Safety, a transparent and practicable method for appropriate use by Member States' competent authorities when they assess the risks of non-food consumer products [RAPEX Guidelines].

In the scope of the RAPEX Guidelines, risk is *"the combination of the severity of possible damage to the consumer and the probability that this damage should occur"* [i.31].

While the RAPEX Guidelines provide ordinal scales for the severity of harm and the probability of the occurrence of the arm scenario (through the foreseeable lifetime of the product) and a table that classifies the risk of harm on the basis of combinations of points on those scales, these neither apply nor translate in a straightforward manner to scenarios where the product is not a consumer one, the subject that bears the harm is not a consumer, or the harm does not involve physical injury.

# 7 Challenges in risk assessment

## 7.1 General challenges

As discussed so far, an understanding of how exactly risk assessment methodologies should be applied in the context of cyber issues under the NLF is largely missing.

The business objective of a risk assessment is to estimate levels of exposure to the likelihood of loss and the impact of loss, so that informed decisions on how those risks can be managed can be made at the appropriate level of the organization [i.22]. In the current risk assessment landscape, this entails a number of challenges:

- It is not possible to compare the results of different risk assessments (e.g. between different organizations or even between different scenarios within a single organization) in a reliable manner. In turn this renders comparisons of risk posture virtually impossible and the analysis of trends in regard to risk and its treatment across different organizations and industries impractical.
- It is not straightforward to determine which criteria would objectively differentiate risk assessment methodologies in a manner that would enable selection of the most effective and/or efficient methodology in a given context.

Another challenge lies in the significant variance that characterizes the discourse about cyber risks. While several standards about risk management exist at a national and international level, the adoption of a common standard set of terms and practices is still far from universal.

The lack of a "lingua franca" that covers the entire domain of concerns about cyber risks is probably the most significant deterrent to progress in the area of cyber risk management.

Taxonomies help those who study a certain body of knowledge to describe and define the problem space. This enables alignment within a group of practitioners and greatly facilitates communication to stakeholders that are not familiar in the matter or its practices. A taxonomy provides the means to categorize - and thus organize - information, to increase the effectiveness of communication, and to develop effective standards [i.23].

Perhaps one of the most significant issues with modern risk assessment frameworks is that they do not provide the assessor with an understanding of how to create scale, or the logical implications of their use of measurements in the context of the chosen scale [i.22].

This poses far-reaching challenges, given that particular aspects of risk may be contingent upon specific practices, particularly in regard to vulnerability disclosure processes [i.41], where uniform measures of assessment are not always readily available across different sectors and even economic sizes.

As a result, different assessors may address these issues in different ways. Such variance is not necessarily conductive to competition forces and thus may lead to a problematic divergence in the market and an unworkable lack of consensus among stakeholders.

## 7.2 Challenges that arise under the NLF

Notably these challenges arise due to the state of risk management practice in the industry overall and regardless of the NLF. However, when cyber risks are put in the scope of harmonised standards, whether as a predicate upon their development phase or as an aspect of their application, these challenges become critical. This is because the primary purpose of harmonised standards is to offer a scalable, relatively frictionless path that stakeholders can follow for the placement of products in the EU single market. Without harmonised standards, it is highly doubtful that technological innovations continue to flow in the EU Single Market at the same pace or at the same price points.

Another challenge concerns what is perhaps the most critical aspect of a risk assessment: the correct identification of its scope. Typically, in the context of the NLF, the scope of the risk assessment is set by the respective legislative acts that establish the products and/or services they apply to. However, the text in the legislative acts may oftentimes use terms that are rather ambiguous and require further interpretation. This impacts upon the correct identification of the scope for a risk assessment, where the said legislative acts, or other normative texts (e.g. standardization requests) require one. The additional interpretative step means that, unless a common norm to which all stakeholders abide exist, the scope of the risk assessment may differ between different assessors and lead to different results.

To achieve citation in the Official Journal of the European Union, harmonised standards undergo further scrutiny by the European Commission. For any given legislative act under the NLF, one or more standardization requests list the harmonised standards that are relevant. However, standardization requests may - in addition to the requirements found in the respective legislative acts - introduce specific requirements upon harmonised standards. In the past such requirements had an impact on the development process of harmonised standards, as regards its risk assessment aspects. Given the lack of alignment in the practice of risk assessment across the industry and the large variance in the application of risk management in different organizations, these additional requirements introduce a risk to the citation of said harmonised standards in the Official Journal of the European Union.

## 7.3 Challenges that arise through current legislation

### 7.3.1 Cyber Security Act (CSA)

The CSA [i.46] does not provide further details on the risk assessment methodology that should apply on particular schemes under the CSA. While that may be intentional and, where the scope of different CSAs does not overlap, practically applicable, it does not guarantee a consistent assessment of risk across CSA schemes. Hence while CSA schemes may be developed so that a particular product, service or process that falls under a CSA scheme does not fall under any other CSA scheme, there is no guarantee given by the CSA [i.46] that the risk that these products, services or processes carry has assessed in a consistent manner across CSA schemes.

Evidently, this leaves room for the case where risks are considered in the development of a CSA scheme, but are, in fact, insufficiently addressed. And where CSA schemes overlap, there is clearly no guarantee that the respective risk assessments (that determine the respective assurance level) are mutually consistent as regards the level of risk.

### 7.3.2 Radio Equipment Directive (RED) Delegated Regulation

Delegated Regulation 2022/30 [i.18] does not impact Directive 2014/53 [i.16] on any aspect relevant to risk. However, the respective Standardization Request [i.20] requires that the development of the respective harmonised standards follows the iterative process of risk assessment and risk reduction.

Consequently, the development of the said harmonised standards should employ a method to assess the risks relevant to the Art. 3(3)(d, e, f) of Directive 2014/53 [i.16] and confirm that each particular security measure achieves a risk reduction. However, there is not guidance given as to which particular method (or methods) of risk assessment would be appropriate for this exercise.

### 7.3.3 Artificial Intelligence Act (AI Act)

To accommodate emerging uses and applications of AI, the European Commission may expand the list of high-risk AI systems used within certain pre-defined areas, by applying a set of criteria and risk assessment methodology [i.28]. However, no further details on these criteria and the risk assessment methodology are given.

The single other mention of risk classification for AI systems found in the AI Act concerns standalone AI systems (i.e. high-risk AI systems other than those that are safety components of products, or which are themselves products). For standalone AI systems, the AI Act considers it appropriate to classify them as high-risk if, in the light of their intended purpose, they pose a high risk of harm to the health and safety or the fundamental rights of persons, taking into account both the severity of the possible harm and its probability of occurrence and they are used in a number of specifically areas specified in the AI Act.

However, again, no additional details are given about the methodology that one should apply to determine whether a risk of harm to the health and safety or the fundamental rights of persons is high or not.

### 7.3.4 Cyber Resilience Act (CRA)

A particular challenge that CRA [i.27] brings results from its scope that includes product's entire lifecycle (i.e. in planning, design, development, production, delivery and maintenance phases). It is not yet clear which considerations would most appropriately and effectively inform the assessment of risk over such a wide scope.

This is not only due to the amount of fragmentation that characterizes the treatment of risk in ICT (i.e. in terms of the distribution of responsibilities across production, operation, maintenance and decommission), but also due to the combinatorial nature of modern ICT systems.

CRA [i.27] requires that products in its scope fall in either of four (4) classes in terms of risk with a specific list of categories (see Annex III in CRA) for two (2) of those classes of risk. The inherent difficulty of an accurate (or even representative) classification aside, modern ICT comprises immense volumes of components whose risk cannot be identified in isolation - only in the content of the ICT system (and environment) they become a part of.

These challenges are further perplexed by the evolving nature of the vulnerability landscape and the - potentially high - differences in the risk posture of the use cases that ICT components end up in.

Again, no details are given about the methodology that one should apply to determine whether a risk of harm to the health and safety or the fundamental rights of persons is high or not.

## 7.4 Conclusion

As part of the outcome of the risk assessment done by an economic stakeholder, harmonised standards that are applied to address the risks identified are indicated.

A common understanding of how obligations in relation to risk assessment translate into steps of an approach that can be applied in common across different stakeholders is a key step in untangling several of the challenges identified.

The rest of the present document focuses on what steps would be essential to such an approach.

# 8 Landscape of standards and guidelines on risk

## 8.1 Foundations

### 8.1.1 Introduction

This clause presents prominent standards in the area of risk assessment. These standards are often part of a family of standards or a wider coherent group of guidelines.

It is paramount that the fundamental principles that inform the treatment of risk should be clearly understood by all stakeholders. In that regard, the work of the DoCRA Council that authors, maintains, and distributes standards and methods pertaining to the analysis and management of risk are relevant. More specifically, the Duty of Care Risk Analysis [i.21] standard that presents principles and practices for analysing risks so that risk assessors equitably evaluate the interests of all parties potentially affected by risks.

### 8.1.2 Principles

#### 8.1.2.1 General

The [i.21] standard applies three (3) principles to risk analysis to ensure that the results of the analysis are:

1) Fair to all stakeholders.

2) Appropriate to all parties.

3) Reasonable to the assessor.

Because the [i.21] principles are in alignment to the expectations and the positions historically taken by regulatory stakeholders and the judiciary, they are an important concern to any risk management mandate. Even more so if that comes with a liability exposure.

For the same of completeness, the principles in [i.21] are listed below.

#### 8.1.2.2 Inclusiveness

"*Risk analysis must consider the interests of all parties that may be harmed by the risk*".

- *"Risk evaluations must include the foreseeability and magnitude of harm that may be experienced by any party".*
- *"Risk evaluations must characterize degrees of risk using resilience thresholds. These thresholds must be applied to all factors in a risk analysis so that degrees of risk to different parties may be compared equitably".*
- *"Assessing organizations may indicate the nature of their relationship to the other parties to declare whether they believe they have a duty of care to those parties".*

#### 8.1.2.3 Fairness

"*Risks must be reduced to a level that would not require a remedy to any party*".

- *"Assessing organizations must declare their intention to present risks to themselves and others that a reasonable person would accept as a consequence of engaging in the risk that would not require a remedy".*
- *"Estimations of risks that would be acceptable to other parties may be attained through rigorous estimation, assumption on the part of the assessor, explicit or tacit agreement with other parties, or other means".*

#### 8.1.2.4 Efficiency

"*Safeguards must not be more burdensome than the risks they protect against*".

- *"Assessing organizations must declare their intention to reduce risks using safeguards that are not more burdensome than the risks that the safeguards protect against".*
- *"The assessing organization may compare the total burden to the total risk, or may evaluate alternative controls by comparing incremental burdens to incremental reductions in risk that the alternative control would incur".*

### 8.1.3 Practices

The [i.21] standard declares ten (10) practices that assessors should apply to achieve the said principles. It is possible and appropriate that assessors may develop variations on these practices that effectively support the principles in their particular situation.

1) Risk analysis considers the likelihood that threats could create magnitudes of impact.
2) Tolerance thresholds are stated in plain language and are applied to each factor in a risk analysis.
3) Impact and likelihood scores have a qualitative component that concisely states the concerns of interested parties, authorities, and the assessing organization.
4) Impact and likelihood scores are derived by a quantitative calculation that permits comparability among all evaluated risks, safeguards, and against risk acceptance criteria.
5) Impact definitions ensure that the magnitude of harm to one party is equated with the magnitude of harm to others.
6) Impact definitions should have an explicit boundary between those magnitudes that would be acceptable to all parties and those that would not be.
7) Impact definitions address; the organization's mission or utility to explain why the organization and others engage risk, the organization's self-interested objectives, and the organization's obligations to protect others from harm.
8) Risk analysis relies on a standard of care to analyse current controls and recommended safeguards.
9) Risk is analysed by subject matter experts who use evidence to evaluate risks and safeguards.

10) Risk assessments cannot evaluate all foreseeable risks. Risk assessments re-occur to identify and address more risks over time.

## 8.2 Approaches

In the presence of unknown adversaries, threat modelling and risk assessment are paramount to risk management.

Threat modelling refers to the development and definition of a model that, with sufficient accuracy, represents the actions and behaviours that adversaries may undertake and demonstrate, respectively.

Risk assessment refers to a process of evaluation of the risks that may result through the realization of particular threats, where the evaluation considers the likelihood of those threats and the impacts they may have.

## 8.3 Standards

### 8.3.1 Introduction

Several standardization organizations address risk management and risk assessment. For instance, recommendations (i.e. telecommunications and computer protocol specifications) published by ITU-T address risk issues in the context of telecommunications [i.38] and [i.39]. Other standardization organizations focus on more generic (e.g. process-related) aspects of risk management and risk assessment.

### 8.3.2 Standards on risk management

The ISO Guide 73:2009 [i.1] provides the definitions of 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.

The ISO Guide 73:2009 [i.1] is intended to be used by:

- Those engaged in managing risks.
- Those who are involved in activities of ISO and IEC.
- Developers of national or sector-specific standards, guides, procedures and codes of practice relating to the management of risk.

ISO 31000:2018 [i.2] provides guidelines on managing risk faced by organizations. The application of these guidelines can be customized to any organization and its context.

Thus ISO 31000:2018 [i.2] provides a common approach to managing any type of risk and is not industry or sector specific. ISO 31000:2018 [i.2] can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.

IEC 31010:2019 [i.3] 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 IEC 31010:2019 standard [i.3] provides summaries of a range of techniques, with references to other documents where the techniques are described in more detail.

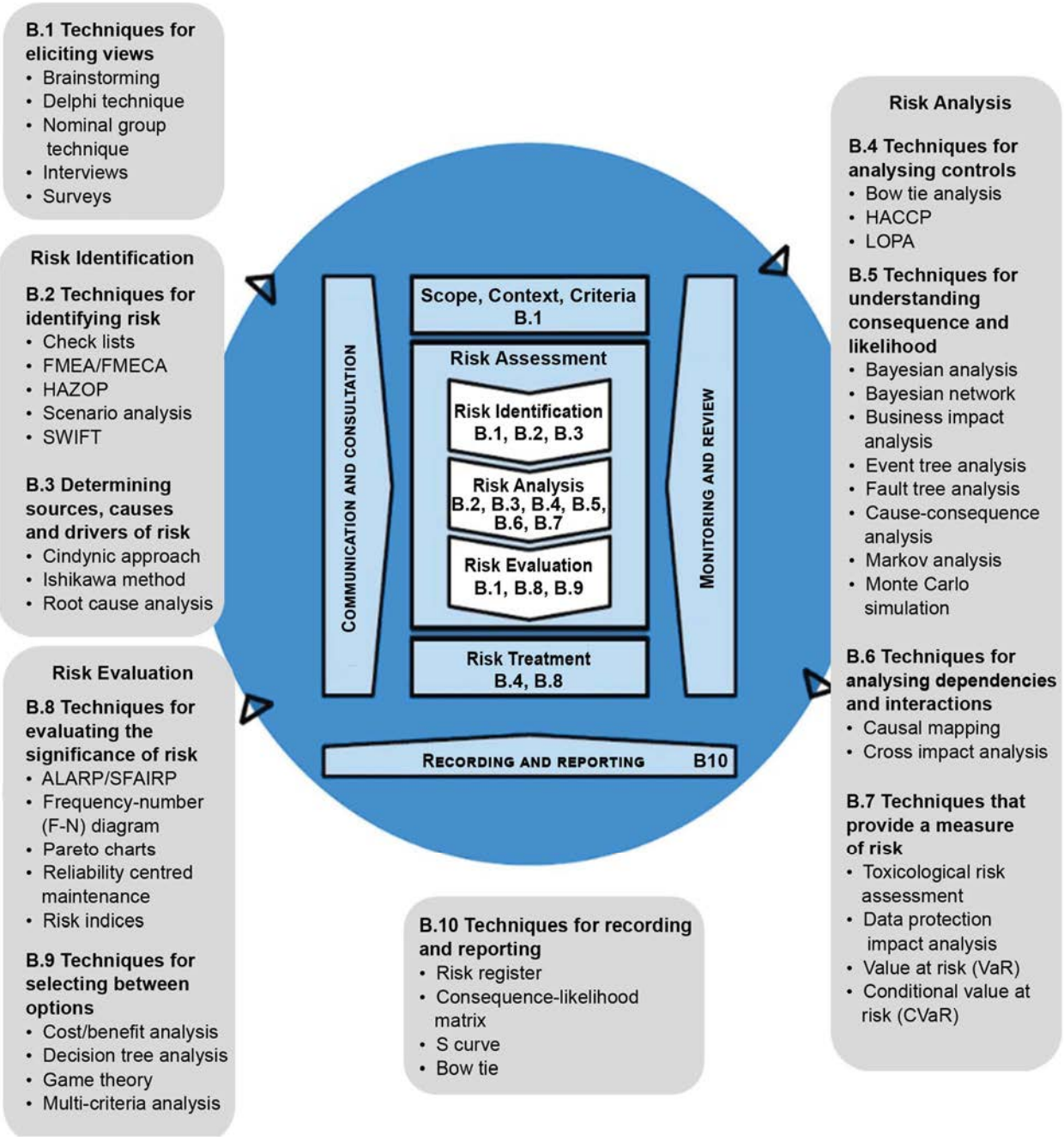


**Figure 1: Application of techniques in the ISO 31000 [i.2] risk management process**

## 8.3.3 Standards on information security

The ISO/IEC 27000-series of standards that are jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) provide best practice recommendations on information security management.

Information security management refers to the management of information risks through information security controls. The latter reside in the context of an Information Security Management System (ISMS).

The ISO/IEC 27000-series of standards are intentionally broad in scope so that they are applicable by a wide variety of organizations. Application of the ISO/IEC 27000-series of standards requires customization to the situation of the particular organization.

The ISMS concept comprises continuous feedback and activities to improve particular qualities of its operation in response to changes in the threats, vulnerabilities and the impacts of incidents.

The ISO/IEC 27000 series of standards includes also standards relevant to risk management:

a) ISO/IEC 27000 [i.5] provides the 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 organization (e.g. commercial enterprises, government agencies, not-for-profit organizations).

b) ISO/IEC 27002 [i.6] provides a reference set of generic information security controls including implementation guidance. This document is designed to be used by organizations:

   i) within the context of an Information Security Management System (ISMS) based on ISO/IEC 27001 [i.43];

   ii) for implementing information security controls based on internationally recognized best practices; and

   iii) for developing organization-specific information security management guidelines.

c) ISO/IEC 27005 [i.7] provides guidance to assist organizations to fulfil the requirements of ISO/IEC 27001 [i.43] concerning actions to address information security risks and perform information security risk management activities, specifically information security risk assessment and treatment. It is noted that ISO/IEC 27005 [i.7] does not provide any specific method for information security risk management, nor any guidance on implementation matters of the ISMS requirements given in ISO/IEC 27001 [i.43].

As regards risk management, the ISO/IEC 27000 series builds on the ISO/IEC 31000 series and adopts the same risk management process as shown in Figure 2.

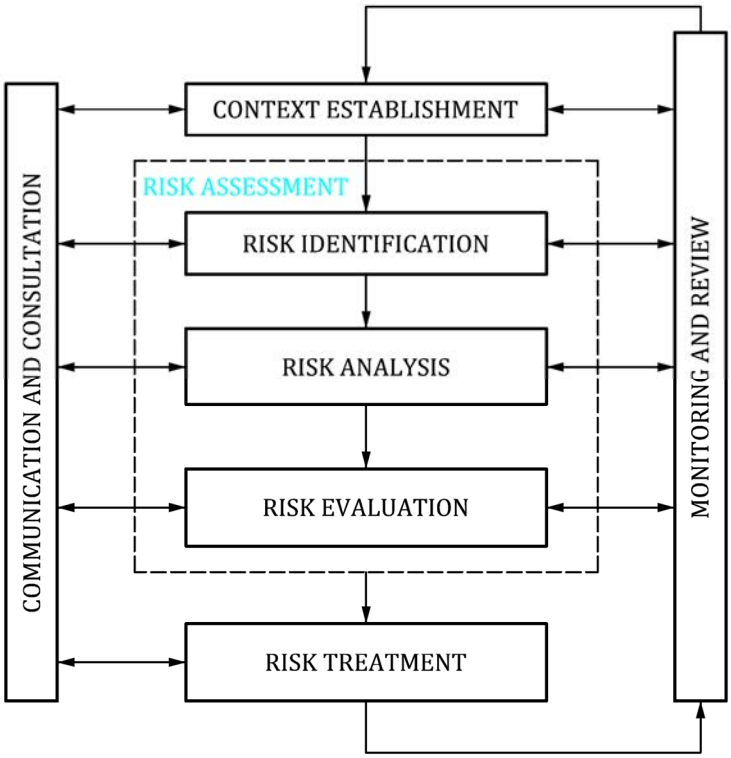


**Figure 2: The risk management process in ISO/IEC 27000 series and ISO/IEC 31000 series**

## 8.4 Methods

### 8.4.1 Introduction

This clause outlines established methodologies that cater for threat modelling, risk assessment, or both.

From a framework standpoint, and for the purposes of the methodologies addressed herein, risk assessment, and the respective threat modelling, take place at the information system tier [i.11]. A risk assessment should, as a minimum, evaluate the anticipated vulnerabilities and predisposing conditions affecting the security objectives of the system (e.g. confidentiality, integrity, availability, etc.) in the context of its planned environment of operation (i.e. its intended use) [i.12].

A risk assessment methodology typically comprises distinct elements (see Table 1).

**Table 1: Elements of risk assessment methodologies**

| Element | Subject | Purpose |
|---|---|---|
| Process | Risk assessment | Assesses the risk |
| Model | Risk | Defines key terms and risk factors<br>Defines relationships between risk factors |
| Approaches | Assessment | Domain of function(s) that evaluates a single risk factor (to a value) |
| | | Domain of function(s) that evaluate combinations of risk factors (to a value) |
| | Analysis | Describes how combinations of risk factors are put under analysis so as to achieve sufficient coverage of the space of concerns at a consistent level of detail |

A risk model provides definitions for the concepts that jointly determine risk and for the relationships that hold between those concepts. Table 2 lists the fundamental elements of a risk model.

**Table 2: Elements of a risk model**

| Attribute | Uncertain? | Note |
|---|---|---|
| Threat | No | A risk model takes an enumeration of threats as given. Threat modelling can produce such an enumeration of threats. |
| Vulnerability | No | A risk model takes an enumeration of vulnerabilities as given. Threat modelling can produce such an enumeration of threats. |
| Likelihood | Yes | A risk model determines the likelihood of particular events. |
| Impact | Yes | A risk model determines the impact of particular events. |
| Risk | Yes | A risk model determines the risk of particular events. |

A security model provides definitions for the concepts that jointly determine the security of the system in question and for the relationships that hold between those concepts. A generic security model ISO/IEC 15408-1:2022 [i.35] and ISO/IEC 15408-3:2022 [i.37] can be seen in Figure 3.

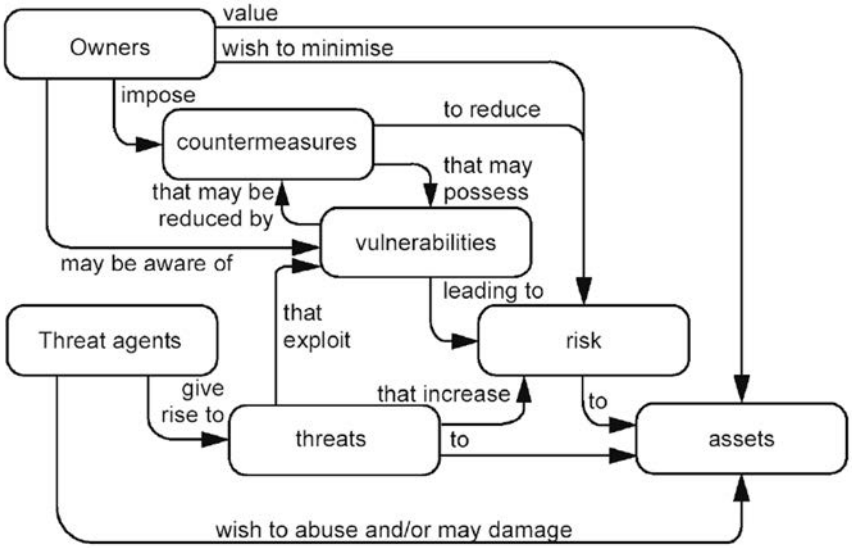


**Figure 3: Generic security model**

### 8.4.2 STRIDE

STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of Privilege) is a threat modelling approach originally developed by Microsoft™.

A model of the system as set in its environment inform the STRIDE process. The level of detail in STRIDE can adapt to the detail of the system's model (i.e. in terms of its elements and the relationships among those elements). STRIDE uses data flow diagrams that depict the flow of data between system entities and the environment of the system when particular events occur.

STRIDE serves primarily as a categorization of general types of threat vectors to consider. Threat modelling in STRIDE starts from the identification of systems and of trust boundaries between those systems as well as to the environment they operate. Opportunities for adversaries are identified by analysing the interactions that take place across trust boundaries. Hence STRIDE focuses primarily on the assets to protect.

### 8.4.3 DREAD

While not a threat modelling method, DREAD complements STRIDE in the sense that DREAD provides a scheme to evaluate and prioritize threat vectors; the latter may be the outcome of STRIDE.

DREAD considers the following properties in the evaluation of threat vectors:

1) Damage - how bad would an attack be?
2) Reliability - how easy is it to reproduce the attack?
3) Exploitability - how much work is it to launch the attack?
4) Affected users - how many people will be impacted?
5) Discoverability - how easy is it to discover the threat?

The evaluation of a threat vector considers its impact; hence DREAD focuses primarily in risk assessment. The measures that DREAD considers (e.g. how "easy", how "much", etc.) reflect the probability distribution that governs particular impacts and, therefore, inform the risk assessment.

### 8.4.4 MITRE ATT&CK

Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) is a framework developed by the MITRE to describe actions that an adversary may take. Its focus is on the actions of an adversary in the course of establishing initial access to its target environment via a successful exploit.

The primary purpose of ATT&CK is to inform defence stakeholders in the tactics that an adversary may exhibit after a successful exploit. ATT&CK defines the following tactics:

1) Reconnaissance
2) Resource development
3) Initial access
4) Execution
5) Persistence
6) Privilege escalation
7) Defence evasion
8) Credential access
9) Discovery
10) Lateral movement

11) Collection

12) Command and control

13) Exfiltration

14) Impact

The evaluation of ATT&CK considers adversary behaviour after initial access to its target environment; hence ATT&CK focuses primarily in risk assessment.

### 8.4.5 Attack Trees

Attack trees illustrate ways that a particular attack against a particular asset may take place. An attack tree is a logical multi-level diagram that complies with a tree structure of a single root node, one or more branches that originate from each node and terminate in a single child node, and every child node having exactly one branch that terminates to it.

Attack trees considers the ways that an adversary may mount an attack against a particular system; hence attack trees focus primarily in threat modelling.

### 8.4.6 Data-Centric Threat Modelling

The approach in NIST SP 800-154 [i.40] focuses on threat modelling for a data-centric system. It thus focuses on the security of particular instances of data within the scope of a system.

The data-centric threat modelling includes the following stages:

1) Identification and characterization of the system and the data.

2) Identification and selection of the attack vectors to include in the threat model.

3) Characterization of the security controls that mitigate the attack vectors.

4) Analysis of the threat model.

### 8.4.7 Threat Vulnerability and Risk Analysis (TVRA)

TVRA is used to identify risk to the system based upon the product of the likelihood of an attack, and the impact that such an attack will have on the system. TVRA provides a means of documenting the rationale for designing security countermeasures in a system by application of a systematic method, and by using part of the method to visualize the relationship of objectives, requirements, and system design and system vulnerabilities.

TVRA requires particular pieces of documentation:

- The system under examination (that includes objectives and requirements).
- The assets of the system.
- How the system fits to its environment.

The primary focus of the TVRA is on the assets of a system where it is necessary to ensure that they can perform their primary function when subjected to malicious attack. The output of the TVRA is a quantified measure of the risks to the assets and a set of detailed security requirements that will minimize that risk.

The depth of the TVRA changes as the system design becomes more detailed. Any change either internal (e.g. by application of countermeasures) or external to the system requires that the TVRA process is redone.

The primary purpose of an ETSI TVRA is to support and rationalize security standardization, and to support and rationalize system design decisions, where the overall objective of the standard is to minimize risk of exploitation and attack of a compliant system when deployed.

The TVRA method addresses the impact of an attack on the system whereas ISO/IEC 15408 [i.35], [i.36], [i.37] primarily addresses the resistance of the system to an attack.

The TVRA method systematically identifies the assets, and the relationships between assets (where the relationship may be considered as an intangible asset) and then for each asset establishes the weaknesses this asset may have, assesses how practical it is to attack this weakness and assesses the resulting risk. More specifically, TVRA proceeds through the following steps:

1) Identification of Target Of Evaluation (TOE)
2) Identification of objectives
3) Identification of functional security requirements
4) Systematic inventory of the assets
5) Systematic identification of vulnerabilities and threat level
6) Calculation of the likelihood of the attack and its impact
7) Establishment of the risks
8) Security countermeasure identification
9) Countermeasure cost-benefit analysis
10) Specification of detailed requirements

The TVRA method follows a classification of threats:

- Interception.
- Manipulation:
  - Forgery.
  - Information corruption.
  - Information loss.
  - Masquerade.
  - Unauthorized access.
- Denial of service.
- Repudiation of sending.
- Repudiation of receiving.

The TVRA method follows a classification of security objectives:

- Confidentiality.
- Integrity.
- Availability.
- Authenticity.
- Accountability.

**Table 3: Summary of threat modelling and risk assessment approaches**

| Name | Scope | | Focus | Note |
|---|---|---|---|---|
| | Threat | Risk | | |
| STRIDE | Yes | No | Asset | |
| DREAD | No | Yes | Risk | Takes threat vectors as given |
| ATT&CK | Yes | Yes | Risk | |
| Attack Tree | Yes | No | Threat | |
| NIST SP 800-154 | Yes | No | Asset | Focuses on data |
| TVRA | Yes | Yes | Risk | |

# 9 Solution space for risk assessment

## 9.1 Characteristics of a good risk assessment methodology

### 9.1.1 Probabilistic

Risk manifests through combinations of events whose occurrence is probabilistic in nature. An analysis of the events that determine risk involves a discussion of potential states, and it commonly involves using information that comes with some level of uncertainty. Hence it is impossible to know the risk in a past, current, or future state with absolute certainty [i.23].

Ultimately, any statement about risk is a statement of confidence that describes the issue at hand on the basis of the evidence available at the time. The treatment of risk on the basis of its probability formulation and through the mathematical instruments available provides the necessary rigor, scrutiny, and structure to the risk analysis process and outcome.

A good risk assessment methodology will lend itself to the development of formulations about risk that are probabilistic and thus assist the identification, analysis, assessment and treatment of risks in a rigorous manner [i.23].

### 9.1.2 Accurate

It is straightforward that a good risk assessment method should deliver accurate results. The use of historical data about events and incidents in comparison to current estimations about the risks of future events can inform the assessment of a particular risk assessment method as regards the accuracy of its results [i.23].

However, whenever appropriate historical data about events and incidents are unavailable (or when they are available but lack in quality) it may be possible to assesses accuracy through other approaches:

- Treatment of risk in a probabilistic manner.
- Elaboration of the particular factors that contribute to the emergence of risk under a particular risk model.

Oftentimes, however, an amount of confusion between accuracy and precision and - unrealistic - expectations about precise results in probabilistic exercises impede the proper estimation of risk. While precision concerns the delivery of results that are "exact, as in performance, execution, or amount", accuracy concerns the ability to deliver correct results, even if those results lack in part in their precision [i.23].

Hence a good risk assessment methodology should achieve accuracy (even if so at a marginal expense of precision).

Due to the inherently probabilistic nature of risk, accuracy may be best attainable through an approach that builds on distributions of estimates (rather than singular estimates) and expresses its results in terms of ranges or distributions.

### 9.1.3 Consistent (Repeatable)

It is straightforward that a good risk assessment methodology should achieve consistent results. This means that independent iterations of the methodology, under identical settings, should yield the same results.

That repeatable results are attainable validates a degree of rigor and logic within the risk assessment methodology and its respective model. Moreover, consistency is a crucial aspect of any approach that would lie under public scrutiny as a candidate for wider adoption in practice [i.23].

### 9.1.4 Defensible

It is straightforward that a good risk assessment methodology should achieve defensible results. This means that, under the scrutiny of logic, results should satisfy an inductive relationship to the risk model, the risk assessment methodology, and its input data [i.23].

This would render the results defensible under logic.

### 9.1.5 Logical

To promote transparency and interpretability under logic, a good risk assessment methodology should use a particular risk model as its basis. A risk model provides a formulation of the relationships between the entities that are relevant to the risk and of the interplay of those relationships as regards the emergence of risk [i.23].

Good risk models provide formulations that are:

- Clear (i.e. straightforward to understand).
- Complete (i.e. cover all the risks that are significant and do not cover insignificant risks).
- Consistent (i.e. yield results that align to each other logically and do not yield nonsensical results).

### 9.1.6 Focused on risk

A good risk assessment methodology should yield results that express risk - exclusively - in terms of the probability of events that give rise to the risk (e.g. in terms of probable frequency of those events), and the probability of impact that those event carry (e.g. in terms of probably magnitude of loss) [i.23].

### 9.1.7 Concise and meaningful

A good risk assessment methodology should yield results that are fit for consumption by its audience. Hence results of a risk assessment should be concise and meaningful to the audience.

### 9.1.8 Actionable

A good risk assessment methodology should inform and support further actions in response to risk. Thereupon, a good risk assessment methodology should make its results available in a manner and format that supports the formulation of actionable plans [i.23].

### 9.1.9 Conclusion

Ideally similar to other security standards cyber security could base the risk assessment on physical measurable values. As for cyber security related risks no physical value is currently known which could give a measure of the cyber security risk, a different method which reduces the subjectivity has to be found. In the following clause an approach is presented.

## 9.2 Fitness and selection of methodologies

### 9.2.1 Categories of approaches

Each threat modelling approach has its particular strong points. Table 4 presents a high-level comparison of threat modelling approaches.

**Table 4: Comparison of threat modelling approaches [i.12]**

| Centre of focus | Description | Comments |
|---|---|---|
| Threat | Models the threat and then applies it to a specific environment and the systems, data and processes it contains. This approach starts with the identification of threats and threat events upon which one develops threat scenarios. | Goes through 1 stage(s) before it is possible to inform further outcomes on the basis of intended use.<br>=> threats => intended use<br>In alignment to the generic security model [i.35]. |
| Asset | Identifies the impacts and the respective assets that are or could be at risk due to threats, characterizes the threats that are relevant to those assets, and, finally, sets the latter in the context of specific systems. This approach starts with the identification of impacts and works backwards to identify events and threats that could cause those impacts. | Can immediately inform further outcomes on the basis of intended use.<br>=> intended use => impacts => assets => threats<br>In alignment to the generic security model [i.35]. |
| Vulnerability | Identifies the vulnerabilities that arise in the scope of a system and the environment it operates in. This approach starts with the identification of predisposing conditions or exploitable properties (e.g. weaknesses, deficiencies, etc.) in the system or the environment in which it operates and works backwards to identify events and threats that could exploit those vulnerabilities and the respective impact that results. | Can immediately inform further outcomes on the basis of intended use.<br>=> intended use => vulnerabilities => threats<br>In alignment to the generic security model [i.35]. |

## 9.3 Prioritization rationale

### 9.3.1 Methodology

Given that information about threats is always incomplete, incorrect, or both, any enumeration of threats is inherent with subjective factors. The extent to which the amount of error that - unavoidably - arises due to the involvement of subjective factors can propagate through the stages of the risk assessment impacts the latter's quality.

In approaches where the focus of the initial stages of the risk assessment is either on threats or on vulnerabilities, errors due the involvement of subjective factors will propagate throughout all the subsequent stages of the risk assessment. In contrast, in approaches where the focus is on assets, the amount error that arises due the involvement of subjective factors will arise in and propagate through later stages of the risk assessment. Consequently, ceteris paribus, in the latter approaches, the amount of error that will propagate, will be lower.

Therefore, from the standpoint that deals with subjective factors and their impact on the presumption of conformity under the NLF, approaches that start from an examination of assets, are preferable to approaches that start from an examination of threats or vulnerabilities. The set of assets is directly and exclusively informed by the definition of intended use under the NLF.

Simply put, in light of market placement under the NLF, it is not advisable to follow an approach that introduces an inherently inaccurate representation of reality in the earlier stages of the risk assessment process.

### 9.3.2 Risk

Any approach to threat modelling and/or risk assessment requires a set of criteria that determine the level of risk for any given combination of threat, asset, vulnerability, impact, and counter measure(s).

In support of the determination of the risk level, the respective definitions of such criteria, and the respective rationale that underpins these, should be available.

From an adversary's perspective, and given that security is primarily driven by economic factors, three factors are paramount:

1) The impact that a particular attack can yield upon the victim(s).

2) The extent to which the impact upon a particular victim further extends to, even if in different ways, other subjects.

3) The marginal cost of mounting the particular attack upon additional victims.

Regardless of what the particular impact a victim suffers under an attack is, the extent to which the impact affects other subjects and the marginal cost of attacking other victims define the social profile of the impact. The latter refers to the impacts that subjects other than the victim are likely to suffer as a result of the attack's success on its original target.

**Table 5: Key aspects of an attack's attractiveness to adversaries**

| Property | Description |
|---|---|
| Impact on victim | The consequences of the attack's success on the victim alone.<br>For instance, a consequence of an attack seeking to leverage the product as a source of DDoS can be a much faster rate of depletion of its power budget, when the latter is finite. Another example of consequence of an attack can be the disruption of a local service of the product (e.g. an NTP client). |
| Scale of threat | The degree to which a particular threat is scalable, in the sense that it can extend, at a minimal additional cost, to any other instance of the product under the same intended use.<br>For instance, a threat exploits a vulnerability in the authentication mechanism between a product and an associated service accessible over the Internet to impersonate the latter towards the former. This kind of threat is scalable to all instances of the product that use the said authentication mechanism. Another example of a scalable threat is one that seeks to abuse the remote software update feature of the product in order to render it (temporarily or permanently) inoperable. |
| Locality of impact | The degree to which a particular impact is locally bound, in the sense that it cannot extend beyond a particular distance from the product that is subject to compromise.<br>For instance, an abusive use of the radio resources (e.g. radio channels, etc.) due to a malware specific to the product. This kind of impact cannot extend beyond the distance where radio reception of the abusive product is possible. Another example of a scalable threat is one that seeks to disrupts a supportive service's ability to serve a set of local devices (e.g. an intermediate CA that generates ephemeral certificates on behalf of product in the local radio network). |

The aspects in Table 5 can serve as priority criteria in the assessment of the level of risk for any given combination of threat, asset, vulnerability, impact, and counter measure(s).

# 10 Solutions

## 10.1 Introduction

This clause proposes an approach that concerns in particular the grey areas and challenges in the context of the risk assessment that were previously described. More specifically, regarding the challenge of conformity claims about a product in the scope of a legislation where multiple alternative interpretations are possible.

And while several legislations require that a risk assessment takes place, the context of the risk assessment is not always the same. The stakeholder that undertakes the risk assessment, the categories of risks considered, and the activities that the risk assessment is meant to inform, vary significantly.

Hence, the following categorization of risk assessment is proposed:

For the ESO's activities:

- Threat analysis to determine the potential threats for the scope of the harmonised European Standard (hEN).
- Sufficiency analysis to evaluate how the developed requirements answer the essential requirements and what is the level of achieved risk reduction.
- Risk based criteria for applicability of each requirement.
- Risk based criteria to determine the appropriateness of each requirement.

For the manufacturer's activities:

- Risk assessment conducted by the manufacturer to determine if the product is in scope of the harmonised standard(s), i.e. if the harmonised standard(s)is applicable for the concerned product.
- Risk assessment conducted by the manufacturer to determine the applicability of individual requirement(s) by the involved parties:
  - 1st party, e.g. manufacturer.
  - 2nd party, e.g. customer.
  - 3rd party, e.g. notified body.
  - Market surveillance authority.
- Product risk assessment conducted by the manufacturer to inform in their demonstration of the product's conformity to the legal requirements.

## 10.2 Property-Based Risk Assessment (PBRA)

### 10.2.1 Introduction

As a risk assessment method, the Property-Based Risk Assessment (PBRA) approach considers properties of the product and its intended environment of use.

The motivation behind PBRA is - specifically - the mitigation of subjective traits that risk assessments carry, as these can cause legal uncertainty under the NLF. PBRA is not meant as a generic risk assessment method applicable widely, but rather as a method to augment risk assessments when cast in the light of the NLF.

The PBRA does not guarantee that a particular solution it yields is a generic solution (to the reproducibility challenge that risk assessments present) beyond the original assumptions (e.g. about risk classes, etc.) based upon which PBRA was applied (to yield this particular solution). However, once consensus on the properties of products that PBRA considers when applied in a particular domain is established, risk assessments based on the solution that PBRA delivers are not only reproducible, but also less subjective.

The PBRA approach relies on a set of prior risk assessments that provide a qualitative risk classification for a set of products. In particular, PBRA:

a) seeks a set of properties that describe the union of these sets of products and their intended environment of use with a focus on essential factors that determine risk (e.g. attack surface, consequences of a security incident, etc.); and

b) seeks to approximate a function that outputs the same risk classification as a reproducible quantitative formulation.

Through the description of products exclusively on the basis of a finite set of essential properties the use of plain language terms about products and their types is waived, as one has no longer to depend on the beholder's subjective interpretation of the terms used to refer to and describe particular products. Everyday terms such as "microprocessor", "gateway", etc. that are commonly used to describe products lack an unambiguous definition. Such terms are subjective and lead to inherent interpretations derived from the assessor's individual experience. Thus different audiences may interpret such terms in different ways, which, in particular scenarios applicable under Union legislation, may be particularly problematic or not even acceptable.

Hence it is paramount that products and their types are described in an unambiguous way, free from the biases that individual experiences bring, so that not only can the type equivalence of different products be assessed objectively, but also that the results are reproducible and not subject to each particular audience's interpretation.

### 10.2.2 On subjective factors and legal certainty

It is known that subjective factors decrease confidence and run counter to an assessment's results being reproducible. Particularly in the cyber domain, the confidence in any risk assessment decays over time - even if all relevant subjective factors where somehow made void. This is due to two factors: The full data set of cyber incidents not being available, and the evolving nature of the threat landscape. The former factor means that the probability and impact of cyber events cannot be computed accurately - only estimated. The latter factor means that risk estimates, however diligent, gradually degrades in confidence as threats actors evolve their techniques and tactics.

NOTE: Risk is commonly calculated as the product of the likelihood that a particular event occurs (e.g. that an adversary discovers and exploits a vulnerability) and the consequences of that event.

Though the evolution of the threat landscape is beyond anyone's control, the treatment of subjective factors in risk assessment is not. Through consensus on explicit steps taken to constrain - or even minimize - estimation errors, one can develop risk assessment approaches that yield reproducible results and thus satisfy legal certainty requirements under the NLF.

The question, of course, is: "*which steps?*" - and "*how does one select the right ones?*".

### 10.2.3 Current practice in harmonised standards

If one reviews harmonised standards for the RED cited in the OJEU and tries to identify which aspects address subjective factors, one aspect stands out: the concept of measurement uncertainty.

In a harmonised standard, assumptions in regard to the acceptable level of uncertainty of measurements are documented (e.g. Figure 4). On this basis, results in the test report of product that claims compliance to the harmonised standard can be interpreted unambiguously. This is instrumental to the support of legal certainty by the respective harmonised standard. To support similar levels of confidence in the cyber domain, an analogous construct is necessary.

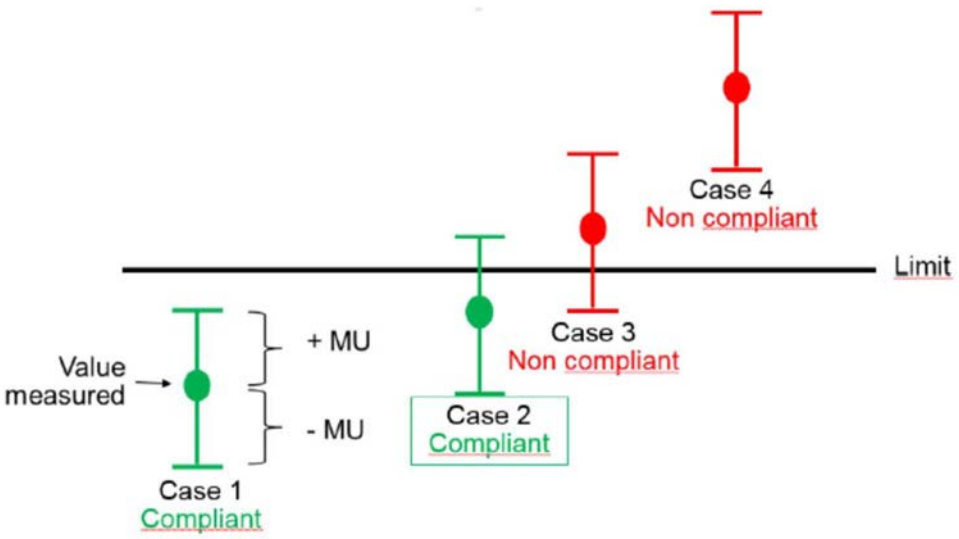


**Figure 4: Application of Measurement Uncertainty (MU) in ETSI EN 302 217-2 [i.44]**

The importance of measurements (i.e. "what" to measure and "how" to measure it) is not unknown to the industry. The OpenGroup notes in its OpenFAIR guidance on risk assessment that "*understanding how the assessment should go about measuring, calculating, and expressing risk is critical to creating a logical, defensible assessment*".

### 10.2.4 Current practice in risk assessment

Because the full data set of cyber incidents is not available, risk assessments in the cyber domain are inherently subjective. In order to reduce the impact of subjective factors, it is common that risk assessments start as qualitative and, as more data about cyber incidents is considered, become more quantitative. Exempli gratia, risk classes may be initially defined qualitatively and iteratively refined to quantitative ones. A qualitative formulation leaves the boundaries of the risk class open to arbitrary interpretations, while a quantitative formulation, although it does not remove all subjectivity, makes such interpretations explicit, thus providing a basis for objectivity. For instance, the subjectivity found in that the (*low risk score*, *high risk score*) boundaries of a risk class are estimates of the actual boundaries of the risk class that one could calculate if given the full data set of cyber incidents. Thus quantitative formulations enable the development of estimation error measures that are comparable, reproducible and verifiable.

Because subjectivity and consensus are inversely proportional to each other, one way to constrain subjective factors is through consensus development. In the context of standardization work, it is possible to address subjective factors through a consensus-driven approach in a Joint Technical Body (JTB) of the European Standardization Organizations that involves experts from all stakeholders and the European Commission. The risk that harmonised standards would be found unfit for purpose in their review by the European Commission mirrors the risk of a restriction in their citation in the OJEU from the perspective of the industry and the European Standardization Organizations.

Therefore, it is paramount that development of the harmonised standards builds upon a quantitative formulation of risk that would classify as an appropriate stable solution and which a consensus-driven approach supports.

## 10.3 Using properties to describe products

### 10.3.1 Product properties

One can discriminate and classify product on the basis of its properties (e.g. type of technology, role it plays, the resources it has available, its operational environment, etc.). Analysis of the product and its use cases can identify such properties.

The product can then be considered by a black box just described by generic properties only referring to the aspects of the essential requirements of a standardization request.

Any other product property which often is implied by the shape, name or other characteristics should be neglected as they are subjective. For instance, lighting equipment may be described by a property which defines the criticality of the controls, A use in an hospital environment is not the relevant aspect while the use for life supporting control in an operation room is relevant versus the use in a patient room.

### 10.3.2 Product classes

Product classes can be thus defined on the basis of the combinations of values that such properties take. Table 6 illustrates an example.

**Table 6: Example of defining product classes on the basis of its properties (2 in this case) and the combinations of values they take (4 in this case)**

| | **Product classes** | | | |
|---|---|---|---|---|
| **Properties** | A | B | C | D |
| Can exchange IP datagrams | Yes | Yes | No | No |
| Includes a hardware root-of-trust | Yes | No | Yes | No |

Using properties and values to describe product is isomorphic to using the Resource Description Framework (RDF) to describe product. RDF is universal in its description capacity (i.e. it can describe anything). Hence, through properties and values, any type of product, however complex, can be described.

NOTE: The isomorphism maps the radio equipment class to the RDF subject, the property names to RDF predicates, and property values to RDF objects.

Given a set of properties and their values, the maximum possible number of product classes that can be described is equal to the number of combinations of the values of the properties. For instance, in Table 6, 4 product classes (A, B, C, D) are defined by 2 properties with 2 values each.

While product can vary significantly, the set of properties and their values can be selected to define a limited set of meaningful types of product.

### 10.3.3 Risk scores

The term risk score in this context refers to the likelihood that an adversary finds a successful attack sufficiently valuable and the respective consequences it would have.

NOTE 1: Other interpretations of the term "risk score" include "a function of likelihood and consequence associated to a risk".

NOTE 2: The expression "an adversary" is understood to mean "at least one type of adversary".

For instance, one can calculate the score of a risk (a device is exposed to) by calculating the likelihood of an incident times Impact or Loss for the stakeholder, while the likelihood is a function ***f***(asset for attacker) times a function ***g***(attack surface).

The higher the risk score, the more valuable a successful attack to an adversary is. For instance, a 4G radio base station would be expected to rank (relatively) high in the risk score scale (as its compromise could impact a large number of customers and their data). Conversely, a IEEE 802.15.1 [i.45] headset would be expected to rank (relatively) low in risk score as its compromise would, in most use cases, impact a single user. Additional factors (e.g. resources of the product, kind of data it conveys, etc.) also impact its risk score.

NOTE 3: The example of Bluetooth radio equipment serves illustration purposes as regards the different levels of risk and protection measures that different types of radio equipment would warrant.

### 10.3.4 Risk classes

A risk class in this context refers to a continuous range of risk score values, over which the likelihood that an adversary finds a successful attack sufficiently valuable varies to a minor degree. In contrast, said likelihood varies significantly across risk classes. Within a risk class, risk scores are indistinguishable as regards this likelihood, while across risk classes they are distinguishably different. Hence a risk class represents a fairly invariant range of the likelihood that an adversary finds a successful attack sufficiently valuable varies to a minor degree.

The estimation of risk considers information about the impact that an event would have and also about the environment of use. Due to the diversity of product, the impact varies significantly, across and within the content of its intended use. For instance, the compromise of customer premises equipment would impact a SOHO customer differently than a residential customer, as their financial concerns differ. In addition, differences in the interests, capabilities and resources of adversaries vary considerably, from the adolescent hacker to the organized groups behind advanced persistent threats. This enables the identification of appropriate security requirements for each risk class and type of risk.

As the estimation of the impact across all possible user scenarios is impracticable, the risk class is taken as a proxy of the risk. This does not restrict the differentiation (as regards risk) that any approach that uses risk classes can support, because, however different the levels of risk would be if one had all the information about user scenarios, it is possible to differentiate risk classes to the same degree.

NOTE: One option would be to map each combination of likelihood and impact to a distinct risk class.

## 10.4 Description of the approach

### 10.4.1 Rationale

It is known that consensus on assumptions underpin the legal certainty (and the respective presumption of conformity) that current harmonised standards afford. In this context, a quantitative risk classification that minimizes the estimation error with strong (e.g. mathematically formulated) guarantees offers a foundation upon which to base confidence in the assessment of conformance.

A foundation of confidence that is common across all the stakeholders of market equipment placement (i.e. product manufacturers, notified bodies, harmonised standards consultants, etc.) is paramount. Lack of it would mean that risk assessments done by different stakeholders can produce different results and, in turn, lead to different interpretations about the requirements that a piece of product should be compliant to. Effectively this would be equivalent to a fragmentation of the EU Single Market in regard to a standardization request, as it would give rise to economic incentives for a race to the bottom.

### 10.4.2 Claims

The Property-Based Risk Assessment (PBRA) approach, as exemplified in this clause, minimizes the probability of a misclassification due to the risk estimation error (subject to specific assumptions for the distribution of the estimation errors).

NOTE: For the current objective function, the assumptions are that the 1st and 2nd order variances of the probability distribution of the risk class boundaries are the same.

### 10.4.3 Objectives

The objective of the PBRA is to constrain and minimize the estimation error, in order to get comparable and reproducible risk evaluation for all concerned types of product.

### 10.4.4 Prerequisites

PBRA requires the consensus of the European Standardization Organizations on:

1) A qualitative classification of product classes into risk classes. Such a classification can be the outcome, whether final or interim, of any risk assessment method chosen by the European Standardization Organizations. It can be an approximate classification, in that it lacks sufficient confidence in its estimation error (as regards the boundaries of risk classes).

2) A definition of properties (and the respective values) to describe a given set of product classes that are sufficiently representative of all the different types of products. Each of these values is associated to a numerical weight that is proportional to the risk exposure the respective values signify. These weights are determined (i.e. calculated) by the PBRA method.

### 10.4.5 Inputs

PBRA takes as input the following information:

1) The total number ($\boldsymbol{N_{PV}}$) of values (where the set of values is taken as the union of all values of all properties) (e.g. $\boldsymbol{N_{PV}} = 15$ in the example in Figure 5).

2) The number ($\boldsymbol{M_{REC}}$) of product classes (e.g. $\boldsymbol{M_{REC}} = 16$ in the example in Figure 5).

3) Matrix $\boldsymbol{A}$ of size ($\boldsymbol{N_{PV}}$) rows x ($\boldsymbol{M_{REC}}$) columns with positive integer values in the **[0, 1]** space. The values in each column of the matrix are determined based on the (property-based) description of the product (see Figure 5 for an example). The semantics of these values are:

   - **0** => the value (of the particular property) does not take part in the description of the product class.

   - **1** => the value (of the particular property) takes part in the description of the product class.

4) List $\boldsymbol{B}$ of size ($\boldsymbol{M_{REC}}$) of tuples ($\boldsymbol{R^{LOW}}$, $\boldsymbol{R^{HIGH}}$) of numbers (see upper section of Figure 5 and rows labelled "High" and "Low" for an example). These are the (quantitative) boundaries for each risk class. These boundaries can be the outcome of a risk estimation exercise (e.g. that considers partial data about cyber incidents, solicits experts' opinion, etc.).

5) Specific objective function $\boldsymbol{f}$ to optimize. Currently the objective function $\boldsymbol{f}$ applied and shown in equation (1) calculates the Euclidean distance of the risk scores of product classes to the respective centroids of the risk classes and the objective is to minimize its value. The formula of this objective function $\boldsymbol{f}$ is shown below where $X(j)$ are the optimization variables that represent the weights associated to property values.

$$f = \sqrt{\sum_{i=1}^{M_{REC}} \left( R_i - \left( R_i^{LOW} + \frac{R_i^{HIGH} - R_i^{LOW}}{2} \right) \right)^2} \quad (1)$$

$$where$$

$$R_i = \sum_{j=1}^{N_{PV}} A(i,j)X(j) \quad \forall i = 1, \dots, M_{REC} \quad (2)$$

$i$ : The product class index.

$j$ : The property value index.

$R_i$ : Risk score of product class *i*.

$R_i^{LOW}$ : Low boundary of risk class *i*.

$R_i^{HIGH}$ : High boundary of risk class *i*.

$R_i^{LOW} + \frac{R_i^{HIGH} - R_i^{LOW}}{2}$ : Middle point in the $(R_i^{LOW}, R_i^{HIGH})$ range of values.

$X(j)$ : Weight for value *j* (i.e. the variables of the function).

NOTE: Other objective functions are possible (e.g. squared root of sums of squares of likelihood and consequence).

### 10.4.6 Outputs

PBRA outputs:

- List ***X*** of size ($N_{PV}$) of weights. These weights represent the relative contribution of each property to the objective function's value. In this particular application, these weights minimize the objective function ***f*** in equation (1) which represents the estimation error. These weights are the ***X(j)*** variables in the objective function in equation (2).

NOTE: The estimation error is meant under the statistical (i.e. probabilistic) definition.

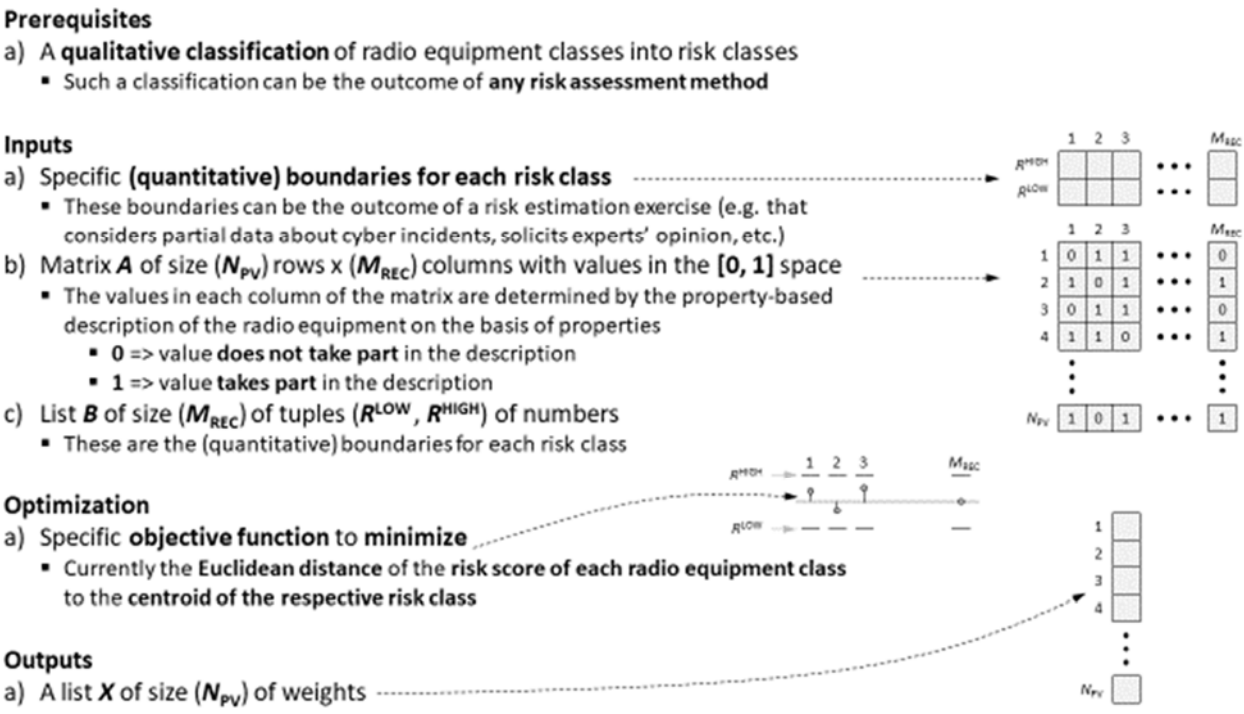


**Figure 5: Summary of the PBRA inputs and outputs**

| | | Risk classes and their boundaries | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | High | 100 | 100 | 84 | 84 | 26 | 26 | 26 | 26 | 84 | 84 | 84 | 84 | 84 | 26 | 26 | 26 |
| | Low | 84 | 84 | 26 | 26 | 0 | 0 | 0 | 0 | 26 | 26 | 26 | 26 | 26 | 0 | 0 | 0 |
| **Values of properties** | | accesspoint_cellular | accesspoint_enterprise | accesspoint_residential | doll_cayla | hearing_aid | microphone | microphone_hub | microphone_repeater | robot_clean | robot_service | smart_camera | smart_door_lock | smart_heart_monitor | zigbee_gateway | zigbee_repeater | zigbee_sensor |
| can_convey_datagram_false | | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| can_convey_datagram_true | | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 1 | 1 | 0 | 1 | 1 | 1 |
| control_by_application_false | | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| control_by_application_true | | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 0 |
| has_ample_computing_false | | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 |
| has_ample_computing_true | | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| has_ample_range_false | | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0 | 1 | 1 |
| has_ample_range_true | | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| has_supportive_role_false | | 0 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 0 | 0 | 1 |
| has_supportive_role_true | | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 1 | 1 | 0 |
| lacks_hardware_rot_false | | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| lacks_hardware_rot_true | | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| power_up_capability_days | | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 |
| power_up_capability_hours | | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 |
| power_up_capability_minutes | | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |

NOTE: The reader may note that all of the significance that properties have is embodied in their values.

**Figure 6: Illustrative application of the PBRA for a specific list of values of properties (blue rectangle), inputs *A* (red rectangle), *B* (green rectangle) and product classes (cells in grey background directly below *B*)**

### 10.4.7 Steps

A practical application of PBRA takes place through the following steps:

1) An analysis of use cases and foreseen environment of use of the product (e.g. by the consensus processes of European Standardization Organizations) that identifies essential differences between product and its operational environment that impact the application of harmonised standard(s).

2) A list of properties (and their values) that describe the different classes of product found in these use cases is identified (e.g. by the consensus processes of European Standardization Organizations). A property has to be orthogonal to each other (i.e. the value of one property should not be a function of the value of other properties).

3) The different classes of product are described through these properties. This is done by enumerating all the different combinations of values for these properties. Each (significantly representative) combination is given a label (i.e. as described in Figure 5) for human readability purposes (e.g. as in Figure 5).

4) The number of risk classes to support is determined (e.g. by a solicitation of experts' opinions, by the consensus processes of European Standardization Organizations, etc.).

5) An approximate risk classification that assigns a risk class to each product class. This can be done through any currently available risk assessment approach.

## 10.5 Iteration steps

### 10.5.1 Preparation

1) An initial analysis of use cases is undertaken, to identify an initial set of product classes that are sufficiently representative (i.e. express commonalities and differences sufficiently) of all types of product in the scope of the harmonised standard(s).

2) An analysis of commonalities and differences of these product classes is undertaken, in order to identify appropriate properties and their values that describe these product classes.

3) An enumeration of all the combinations of values for all properties is undertaken, and an appropriate description is assigned to each of the product classes that each of the combinations of values for all properties represents (e.g. "4G base station", "residential access" point, "Bluetooth headset", etc.).

4) An initial threat analysis and risk assessment is undertaken, in order to establish the prerequisites of PBRA (i.e. the estimation of the risk classes' boundaries and the initial approximate classification of product classes into risk classes).

### 10.5.2 Determination of the solution

The steps of the approach in clause 10.4 are undertaken to calculate the list of weights $\boldsymbol{X}$.

### 10.5.3 Assessment of fitness of the solution

The solution is reviewed for semantic consistency (i.e. as regards the role that particular properties and their value play comparatively to each other in the risk model) as an additional check to the risk classification assumptions:

- If the solution is semantically consistent, the process proceeds to the consensus review (see below).
- If the consensus is unsuccessful, the feedback is analysed and considered in the next iteration of the process.

After a successful review for semantic consistency the process proceeds to the consensus and approval process of the European Standardization Organizations:

- If consensus is successful, the process terminates, and the respective solution is fed to the standardization process.
- If the consensus is unsuccessful, the feedback is analysed and considered in the next iteration of the process.

**The economic stakeholder (e.g. manufacturer, distributor, etc.) perspective**

In placing a product in the EU Single Market, manufacturers are free to choose between three (3) options:

1) A complete description of the product (i.e. using all of the properties standardized for Articles 3(3)(d, e, f)). This would guarantee that the product maps to a standardized risk class) and, to that end, no additional documentation or action is necessary.

2) A partial description of the product (i.e. using some of the properties standardized for Articles 3(3)(d, e, f)). This would not guarantee that the product maps to a standardized risk class) and, to that end, additional documentation and action is necessary.

3) Satisfy an accredited notified body that their equipment (and the respective technical file) meets the legal requirements of the Delegated Act for the RED.

## 10.6 The economic stakeholder perspective

### 10.6.1 Evaluation by a manufacturer according to options 1 and 2

The manufacturer can use the tool (e.g. a spreadsheet) provided within the RED related standard as support for the risk assessment of their product.

When using the tool, for each of the Articles 3(3)(d, e, f) the manufacturer describes the product of concern by selecting a value from the enumeration for each property. For instance, selecting, for the property "Radio interface can convey IP datagrams" the value "YES", and, for the property "Privacy of processed data" the value "Behavioural Personally Identifiable Information".

In the enumeration of each property, each of the values is assigned to a weight, which, is proportional to the risk exposure for that property specifically. By selecting a value, the respective weight is applied (automatically by the tool) in the formula that calculates the risk score for the respective product.

Once this is done for all properties the risk score of the product is calculated by the tool using the formula embedded in the tool and based on the weights (as defined and standardized by the European Standardization Organizations). The formula and weights are not visible to the user of the tool (i.e. the manufacturer or assessor). Hence this works as a black box, where the user is inputting the product characterization and, in return, gets a risk score for their product as a result.

The risk score maps to one of the defined risk classes (e.g. medium). Then the manufacturer (or assessor) looks up the respective clause (i.e. for the "medium") of the harmonised standard for the concerned article (i.e. one of Articles 3(3)(d, e, f)). In this clause of the standard the manufacturer (or assessor) finds the provisions required to be fulfilled by the product.

If the manufacturer choses to omit assignment of a value to a property, then they still get a risk score. However, in this case, the tool applies the weights that contribute mostly to the risk score. The manufacturer can choose to accept this risk score and apply the respective provisions, or, provide a dedicated justification for this property in the context of market placement.

The major advantage of this process is the comparability and the enablement of reproducible and verifiable results in the risk classification - in contrast to a situation where each manufacturer carries out the risk classification on its own interpretation.

### 10.6.2 Summary and Future perspective: areas of possible improvement

In order to ensure a full description of the product, the formula that calculates the risk score should start with the assumption that the risk score is high. As properties are added to the description, they subtract from the high score, ensuring that manufacturers provide a complete description of their product, thus increasing the legal certainty of this method.

Currently, the risk score function is entirely additive. The more complete the description of a piece of product (by its manufacturer) in terms of values for its properties is, the higher the risk score - at least in comparison to a piece of product of the same type whose description by its manufacturer deliberately omits some properties. Thus one might find incentive in fraudulent behaviour that seeks to secure a lower risk score through additional documentation.

NOTE: The degree to which that is achievable does not matter, as manifestation of the fraudulent behaviour depends also on risk posture, which would vary across a population of manufacturers.

To ensure alignment at an incentive level, the risk score function should subtract from a default (highest) risk score. Thus manufacturers of products might find an incentive in describing their product using as many properties as possible, as that would potentially reap the highest reduction in its risk score.

As a property description can be any text (e.g. a Resource Description Framework (RDF) text), a semantic web connection to collect vulnerability information (for instance from ENISA reports) and deduce properties may be a future option for improvement.

## 10.7 Illustrative application

### 10.7.1 Introduction

To illustrate the PBRA approach, the Delegated Regulation 2022/30 under the Radio Equipment Directive (RED) [i.19] and the respective Standardization Request [i.20] is considered. This legislative initiative is the first application of Union harmonization legislation to address cybersecurity and privacy issues [i.17], [i.18]. Moreover, a considerable percentage of the products in the scope of Delegated Regulation 2022/30 would, to the best of our knowledge given the currently available information, classify as products with digital elements in the meaning of the European Commission's proposal for the Cyber Resilience Act [i.27].

Therefore, without prejudice to its application in the context of other legislative initiatives (see clause 5 on "Legislative landscape"), the rest of this clause focuses on products in the scope of Delegated Regulation 2022/30 under the Radio Equipment Directive (RED) [i.19].

The PBRA approach is applied for 3 different concerns in Delegated Regulation 2022/30 under the Radio Equipment Directive (RED) [i.19]:

- Cyber security
- Privacy (and protection of personal data)
- Fraud (or other fraudulent use)

As these concerns are independent of each other, the PBRA approach is applied independently for each of these concerns. This means that, for each of these concerns, the prerequisites, inputs, objectives, and the outputs of the PBRA approach can be different, as the risks that each of these concerns carries are different.

## 10.7.2 Considerations on the suitability of properties

### 10.7.2.1 Introduction

The definition of the properties to use for each these concerns would be done by the European Standardization Organizations through their consensus process. The purpose is twofold:

- To identify and describe all relevant product categories with sufficient granularity.
- To identify and address the types of risks that are related to each concern.

The properties that comply with the PBRA are identified as to be able to describe any piece of product with sufficiently differentiation. Moreover, specific steps of the method are designed so as to yield objective and reproducible results in the risk classification.

Provisions of existing standards can be mapped to risk levels and thus applied on the basis of the risk classification. For each of the concerns above, the properties refer to specific aspects of the threat exposure.

### 10.7.2.2 For cyber security

- The attack surfaces that a product is exposing to an attacker by defining its physical and logical accessibility for an attack (e.g. hardware and software interfaces, physical access, etc.).
- The (computing) capacity of a product to put up measures to defend, prevent and mitigate an attack.
- The criticality of the control application (e.g. service) of the product in the scenarios of its compromise by an attack (in consideration of its usage in a specific environment).

### 10.7.2.3 For privacy

- Degree of privacy of data in the product or transferred by the product.
- Capability to physically disable the access to private data.

### 10.7.2.4 For fraud

- Criticality of payment data.

## 10.7.3 Identification of properties

### 10.7.3.1 Introduction

Looking for properties that could lead to different counter measures, hence requirement levels compared to the level from the risk analysis for cyber security, a separation of the properties in physical properties and intended use properties is needed. Hence this leads to the following list of generic properties.

#### 10.7.3.2 Cyber security

**Properties to determine the attack surface:**

- Radio interface can convey IP datagrams
  - Yes
  - No
- Is under control of an application that executes on other equipment
  - Yes
  - No
- Ample computing capacity for complex defence algorithms
  - Yes
  - No
- Power-up capability
  - Minutes
  - Hours
  - Days
- Ample communication range
  - Yes
  - No
- Lacks a hardware Root-of-Trust
  - Yes
  - No
- Play a supportive role to other product
  - Yes
  - No

In addition, these properties would cover the following specific requirements of [i.20]:

- *"Include elements to monitor and control network traffic, including the transmission of outgoing data".*
- *"Are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards harm to the network or its functioning or misuse of network resources".*
- *"Are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation of vulnerabilities that if exploited may lead to product harming the network or its functioning or the misuse of network resources".*
- *"Protect the exposed attack surfaces".*

**Properties for describing the intended environment of use:**

- Control aspect of the product (Impact/Criticality of service of the device)
  - Comfort

    - Assets
    - Security
    - Privacy
    - Health
    - Safety
- Level of management of the network
    - Managed
    - Unmanaged
- Physical access to device is restricted to authorized persons/entities
    - Yes
    - No

In addition, these properties would cover the following specific requirements of the Standardization Request:

- Implement appropriate authentication and access control mechanisms.
- Is designed to mitigate the effects of ongoing denial of service attacks.
- Minimize the impact of successful attacks.

#### 10.7.3.3 Privacy

**Properties to determine the attack surface:**

- Radio interface can convey IP datagrams
    - Yes
    - No
- Privacy of processed data for eavesdropping
    - No PII (Personal Identifiable Information)
    - Behavioural PII
    - Non-sensitive PII
    - Sensitive PII
- Privacy of processed data for tampering
    - No PII
    - Behavioural PII
    - Non-sensitive PII
    - Sensitive PII
- Local means to deactivate a sensor that affects privacy exists
    - Yes
    - No

In addition, these properties would cover the following specific requirements in [i.20]:

- *"Protect stored, transmitted or otherwise processed personal data against accidental or unauthorized storage, processing, access, disclosure, unauthorized destruction, loss or alteration or lack of availability".*
- *"Implement appropriate authentication and access control mechanisms".*
- *"Are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards data protection and privacy".*
- *"Are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation vulnerabilities that if exploited may lead to unauthorized storage, processing, access, disclosure, unauthorized destruction, loss or alteration or lack of availability of personal data".*
- *"Include functionalities to inform the user of changes that may affect data protection and privacy".*
- *"Log the internal activity that can have an impact on data protection and privacy".*
- *"Allow users to easily delete their stored personal data, enabling the disposal or replacement of equipment without the risk of exposing personal information".*
- *"Protect the exposed attack surfaces".*
- *"Minimize the impact of successful attacks".*
- *"Hand-held mobile telephones with features similar to those of a computer in terms of capability to treat and store data (smartphones) to which the essential requirement set out in Article 3 (3) (e) becomes applicable pursuant to Delegated Regulation…., permit the deployment of solutions for the provision of services regulated by Regulation (EU) No 910/2014; all their hardware components that would permit these solutions and services to comply with the security requirements regulated by the framework set by Regulation (EU) No 910/2014 shall be accessible by that service".*
- *"Radio equipment designed or intended exclusively for childcare and radio equipment covered by Directive 2009/48/EC child radio equipment, as defined in Article 1 of Delegated Regulation…, to which the essential requirement set out in Article 3 (3) (e) becomes applicable pursuant to that Delegated Regulation, avoid unauthorized communications or interactions to their user".*
- *"Smart meters used for decentralised smart grids in the field of energy and 5G network equipment used by providers of public electronic communications networks and publicly available electronic communications services within the meaning of in Directive (EU) 2018/1972 to which the essential requirement set out in Article 3 (3) (e) becomes applicable pursuant to Delegated Regulation…, maintain the high level of security requested at national level".*

#### 10.7.3.4 Fraud

**Properties to determine the attack surface:**

- Radio interface can convey IP datagrams
  - Yes
  - No
- Sensitivity of payment data for eavesdropping
  - None
  - Non-sensitive
  - Sensitive
- Sensitivity of payment data for tampering
  - None

- Non-sensitive
- Sensitive

In addition, these properties map to the following specific requirements of [i.20]:

- Protect stored, transmitted or otherwise processed financial or monetary data against accidental or unauthorized storage, processing, access, disclosure, unauthorized destruction, loss or alteration or lack of availability.
- Implement appropriate authentication and access control mechanisms.
- Are provided, on a risk basis, with up-to-date software and hardware at the moment of placing on the market that do not contain publicly known exploitable vulnerabilities as regards financial or monetary data.
- Are provided with automated and secure mechanisms for updating software or firmware that allow, when necessary, the mitigation vulnerabilities that if exploited may lead to unauthorized storage, processing, access, disclosure, unauthorized destruction, loss or alteration or lack of availability of financial or monetary data.
- Log the internal activity that can have an impact on financial or monetary data.
- Protect the exposed attack surfaces.
- Minimize the impact of successful attacks.

### 10.7.4 On constraints and the use of values and weights

Over all of the properties defined, the definition of the values (and the respective weights) for each of the concerns above, would be done by the European Standardization Organizations.

Specifically, the determination of the weights utilizes a Constraint Satisfaction Problem (CSP) formulation with an optimization objective (e.g. the objective function ***f*** as shown in equation (1) in clause 10.4). The constraints that are part of the CSP are determined through the consensus process of the European Standardization Organizations.

These constraints are designed in accordance to the respective use cases, in order to get a CSP formulation with at least one solution. The numerical weights in these solutions reflect and depend on the set of properties, how their values reflect upon risk, and the set of product classes.

For instance, when it comes to considering the quantitative classification of a particular class of product to a particular risk class: A constraint upon the risk score of the particular class of product within the boundaries of the risk class (i.e. $R^{LOW} < Risk\ Score < R^{HIGH}$) models this classification.

Subject to the analysis and consensus of the European Standardization Organizations, additional constraints may be defined and included in the CSP formulation (e.g. to model particular aspects of risk that particular properties may entail).

### 10.7.5 Mapping of the Requirements to risk classes

The set of properties as described above should allow for a mid-level model of product. The relatively small set of risk classes (so that one does not have to map the provisions of existing standards to too many risk classes) should then be sufficient to determine on which risk class each product class should fall (as a range of values that the risk score should fall into).

This step would be within the remit of the ESO that would undertake the application of the approach.

### 10.7.6 Conclusions

This clause has demonstrated the applicability of the PBRA method for a real-life scenario that involves a modern legislation with a wide range of products in its scope. The ESO environment that provides well-structured processes to establish consensus among multiple participants is the ideal setting in which PBRA can be applied.

However, it has been repeatedly observed that, even in the light of consensus within the ESO work groups, consistency and reproducibility of risk assessment outcomes are not a given, as even subject matter experts are not entirely free of bias in their assessments.

PBRA has been designed to address explicitly the limitations that, in the light of cybersecurity requirements, bias and other subjective factors raise in the process of placing ICT products in the EU Single Market. PBRA enables market stakeholders to bring their particular expertise and experience to the ESO table and filter out biases that would otherwise lead to inconsistent outcomes.

# Annex A:
# On the appropriateness of tests

## A.1 Introduction

It follows from the discussion so far that tests under the NLF should have particular properties. Table A.1 lists important properties for any kind of test that would aspire to provide sufficient confidence in support of market placement.

**Table A.1: Important properties of a test**

| Property | Description |
|---|---|
| Clarity | A test should specify all the parameters and their ranges that constitute each condition under which the test may take place. |
| Validity | A test should assess only the scope it has been designed to assess (i.e. the scope of the test should match the scope of the test subject). |
| Conclusiveness | A test should always result in exactly one outcome (out of all possible outcomes). |
| Reliability | A test should result in the same outcome under different actor(s) of the same type (e.g. different testers). |
| Economics of repeatability | It should be economically realistic to establish the conditions necessary to repeat a particular test under a given set of conditions. Establishment of the conditions should be possible under a scalable cost model (i.e. any additional costs that are due to the establishment process should be reasonable). |
| Consistency | Repetition of a particular test under the same conditions should always result in the same outcome. |
| Objectivity | A test should result in the same outcome when conducted under the same conditions by different operators (e.g. testers) of comparable competence. |

An important observation is that a test falls into either of the following classes:

a) Tests free of subjective factors

b) Tests with subjective factors

## A.2 Tests free of subjective factors

### A.2.1 General

These are tests that do not involve an element of human assessment.

### A.2.2 Tests that assess the existence of a value

Examples include:

- Assessing product documentation, packaging, and casing for the existence of particular properties (e.g. "Yes" or "No" inputs in response to a question regarding the product, etc.):
  - An example concerns properties of content expected in user documentation, such as security guidance, data protection policy, vulnerability disclosure policy, etc.
  - Another example concerns presence and properties of a label present on the device casing.

- Assessing the existence of a function to achieve a particular outcome:
  - An example is a provision stating that *"where a user can authenticate against a device, the device shall provide to the user or an administrator a mechanism to change the authentication value used"*.
  - Another example is a provision stating that *"the device shall have a secure element"*.
- Assessing that invocation of a particular function with specific inputs yields the expected results (e.g. a list of open network ports as produced by the result of a network scan under a specific scenario).

# A.3 Tests with subjective factors

## A.3.1 General

These are tests that involve an element of human assessment.

## A.3.2 Tests that assess the sufficiency of a feature for a given purpose

Examples include:

- Assessing that a given set of mitigation measures (e.g. the detection of brute-force attacks on an authentication mechanism) provides the desirable level of assurance against particular risks.
- Assessing that the implementation of a particular cryptographic function passes the state-of-the-art benchmark for cryptographic functions. The state-of-the-art is, in general, a moving target, in terms of the universality of any acceptable definition for it. Consequently, in any given time and context, a subjective assessment ensues, to determine what qualifies as state-of-the-art.
- Assessing that the implementation of a particular function is done in a manner appropriate for a particular concern:
  - An example is a provision stating that *"the confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage"*.

## A.3.3 Tests that assess universality properties over a property

Examples include:

- Assessing that a particular password generation mechanism produces passwords that are universally unique across all the instances that employ the said mechanism. This kind of assessment requires enumeration of all instances, which, inherently, does not scale economically as an exercise.
- Assessing that a particular implementation is free of vulnerability (e.g. through penetration testing or fuzzing). Such assessment is limited by factors such as the time available to perform the test, the expertise of the testers, and ability of algorithms to cover a given problem space.

## A.3.4 Tests that comprise negation clauses

Examples include:

- Assessing that invocation of a particular function against any inputs does not yield any undesirable result (e.g. that submission of any SQL statement towards a database frontend interface does not result in any kind of malfunction of the respective process). Typically, the set of all possible inputs is economically unrealistic to enumerate fully during the test.

- Negation clauses (e.g. "*does not*", "*shall not*", etc.) typically express an assertion that a condition should not hold. Without a clear definition of the circumstances under which the said condition should not hold, it is economically infeasible to enumerate all possible circumstances and carry out the test for each. Even in the case that the circumstances are clearly defined, they are inevitably a subset of the larger set of all possible circumstances. Hence, an assessment should be made, on whether the circumstances defined are sufficient for the level of confidence sought given the resources available. Simply put, because lack of evidence does not constitute evidence of lack, if an assertion of lack of a property is sought (i.e. a negation clause), a decision about what qualifies as sufficient evidence for said lack is unavoidable. Thus, subjective factors come into play.

# A.4 Comparison of subjective and non-subjective tests

Figure A.1 summarizes in an illustration how the properties in Table A.1 classify as tests free of subjective factors and tests with subjective factors.

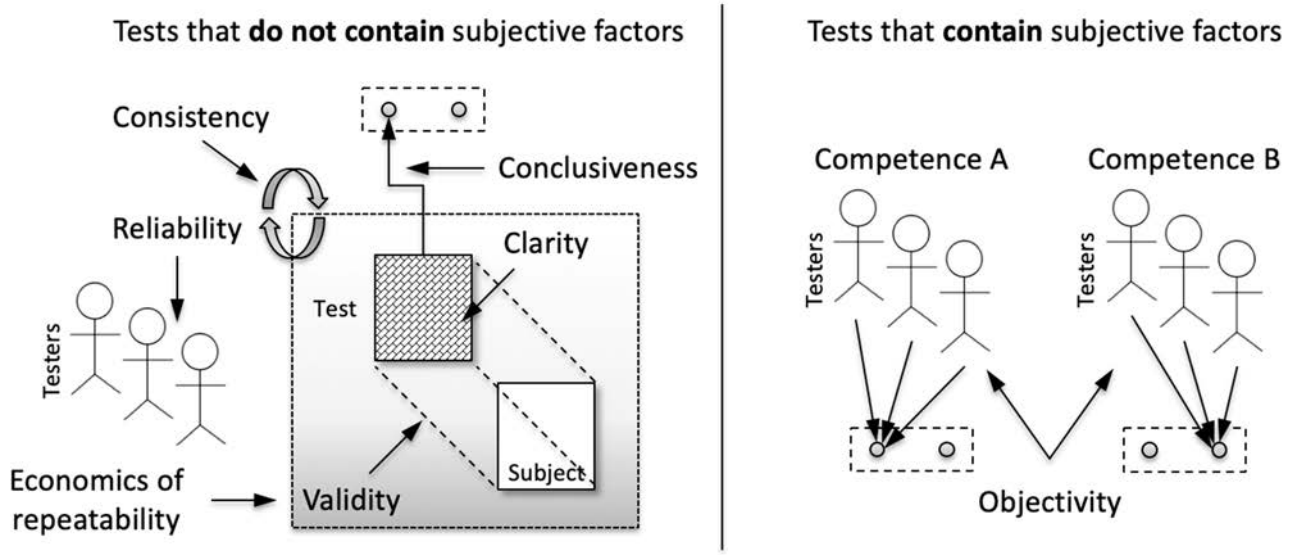


**Figure A.1: Key properties of tests**

# A.5 Important considerations on tests

## A.5.1 Introduction

Procedures applicable in the context of conformity assessment that consider the product and its documentation may take place under the NLF. However, there are some limitations as to what conclusions can be drawn from these procedures, particularly with regard to cybersecurity assurances.

## A.5.2 Aspects of the product that are amendable to tests

Of particular concern are tests that rely on observations of a product's externally visible behaviour to draw conclusions about information that is beyond the field of observation (e.g. internal to the product). These tests while may seem free of subjective factors, but they are in fact not so.

Examples include:

- Assessing that the interaction between a session client and a session server, as observed through a network analyser, meets a particular security requirement.

- Assessing that the network behaviour of product, as observed through a network analyser, meets a particular security requirement.
    - An example is that a product establishes communications providing confidentiality protection, integrity protection, and mutual authentication of peers.
    - Another example is that the product uses cipher suites providing for perfect forward secrecy.

These tests are only seemingly free of subjective factors, as a closer examination reveals. When a tester observes the exchange of protocol messages between systems, there are limited conclusions that can be drawn. For instance, it may be concluded that the exchange of protocol messages and values is aligned to the protocol's specification. However, this does not automatically mean that the information that resides within these systems has been affected as it should have according to the protocol's specification. For instance, protocol emulators work that way, showing alignment to a protocol's specification externally, without fully implementing the actions prescribed by that specification internally.

Assessing the application of confidentiality protection (i.e. encryption) is another area where observation of external behaviour supports limited conclusions. For instance, observing the exchange of particular protocol header values (e.g. cipher suites numbers/codes, etc.) in a security protocol does not guarantee that the respective options have indeed been applied in the subsequent exchange of data. An encrypted piece of information, as observed in the data traffic exchanged (e.g. using a protocol analyser), is entirely unintelligible. And that's how it is supposed to be, so that deciphering the original content is prohibitively difficult for malicious actors. Unfortunately, this also means that, without additional information, a tester is unable to ascertain that confidentiality protection has indeed been applied, or that the encryption parameters employed are indeed the ones prescribed. Any such conclusion requires either additional information, or for the tester to make an assumption about the sufficiency of observations as a basis for that conclusion. Hence tests based on observations of externally visible behaviour, when employed in support of conclusions regarding internal properties, classify as tests with subjective factors.

Moreover, these kinds of tests require the involvement of the cognitive processes of a dedicated tester:

- Assessing that the product is built upon components that provide a set of security properties, based on the identification of said component and reliance on the technical documentation (or, for a higher level of assurance, a security certificate) provided by the component supplier.
    - An example is to assess that a CPU or MCU provides a True Random Number Generator (TRNG) or a Cryptographically Secure Pseudorandom Number Generator (CSPRNG).
    - Another example is to assess that the product uses an operating system that provide a set of features relevant for security, such a privilege separation.

Privilege separation is a supportive measure of security, but does not by itself contribute to stronger security, unless explicitly employed. To understand this, consider the classic security recommendation to organize applications according to the minimum privileges they need and assign them privileges accordingly. However, only applications that should have been designed and developed in alignment to the operating system's privilege model can support such an organization. In addition, the privileges should have been properly configured at the operating system level. Without these steps, it is impossible to separate privileges between different applications, even though the operating system has the capacity.

It should be noted that, while the test of existence (e.g. of a privilege separation capability) considers the operating systems scope, meaningful assurances of security require consideration of the combined scope of the operating system and the application. Hence this is another example of drawing conclusions beyond the field of observation of the test.

### A.5.3 What is currently testable under the NLF?

It follows from the discussion above that tests free of subjective factors are directly applicable under the NLF. On the other hand, tests with subjective factors, to be directly applicable under the NLF, require criteria of sufficiency.

**Table A.2: Example tests that are directly applicable under the NLF**

| Tests that assess the existence of a value |
|---|
| a) Assessing the documentation, packaging, casing, or other physically inspectable aspect of the product for the existence of a particular value. |
| b) Assessing the existence of a function. |
| c) Assessing that invocation of a particular function with specific inputs yields the expected results. |

**Table A.3: Example tests that require criteria of sufficiency to be directly applicableunder the NLF**

| **Tests that assess the sufficiency of a feature for a given purpose** |
|---|
| • Assessing that a given set of mitigation measures (e.g. the detection of brute-force attacks on an authentication mechanism) is appropriate for a particular kind of threat.<br>• Assessing that the implementation of a particular cryptographic function passes the state-of-the-art benchmark for cryptographic functions.<br>• Assessing that the implementation of a particular function is done in a manner appropriate for a particular concern. |
| **Tests that assess universality properties over a property of the test's subject** |
| • Assessing that a particular password generation mechanism produces passwords that are universally unique across all the instances that employ the said mechanism.<br>• Assessing that a particular implementation is free of vulnerability (e.g. through penetration testing or fuzzing). |
| **Tests that comprise negation clauses** |
| • Assessing that invocation of a particular function against any inputs does not yield any undesirable result (e.g. that submission of any SQL statement towards a database frontend interface does not result in any kind of malfunction of the respective process). |

# Annex B: Bibliography


- ETSI TR 103 880: "Study into the challenges of developing harmonised standards in the context of future changes to the environment in which products are being developed and operated".
- European Commission: "Guide to the Radio Equipment Directive 2014/53/EU".
- European Commission: "A European Approach to Artificial Intelligence".
- European Commission: "General Data Protection Regulation (GDPR)".
- European Parliament Research Service (EPRS): Briefing on "Understanding EU data protection policy".
- European Commission, Working Party 29: "Guidelines on Data Protection Impact Assessment (DPIA)".
- ETSI EG 203 251: "Methods for Testing & Specification; Risk-based Security Assessment and Testing Methodologies".

# History

| Document history | | |
|---|---|---|
| V1.1.1 | December 2023 | Publication |
| | | |
| | | |
| | | |
| | | |