ETSI TR 103 990 V1.1.1 (2024-03)

Cyber Security (CYBER);
Standards mapping and gap analysis against regulatory expectations

Reference

DTR/CYBER-00111

Keywords

CRA, Cybersecurity, regulation

ETSI

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

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

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

Important notice

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

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

The present document provides a standards gap analysis against the regulatory expectations of a number of extant, planned, or in development, regulatory instruments in order to identify where existing standards can be used in support, or where new standards are required to enable regulatory conformance. The primary focus of the present document is the Cyber Resilience Act [i.1] with some consideration of the NIS2 Directive [i.2] and the Cyber Security Act (CSA) [i.3].

NOTE 1: The mapped standards listed in clause 2, whilst they are not directly applicable to the application of the present document, are identified as satisfying in whole or in part, one or more of the regulatory expectations identified.

NOTE 2: Matters related to EU policy are not addressed by the present document.

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] Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 (Cyber Resilience Act (CRA)).

[i.2] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[i.3] 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).

[i.4] Supporting documentation for the CRA.

[i.5] New Legislative Framework.

[i.6] Regulation (EU) No 1025/2012 of the European Parliament and of the Council of 25 October 2012 on European standardisation, amending Council Directives 89/686/EEC and 93/15/EEC and Directives 94/9/EC, 94/25/EC, 95/16/EC, 97/23/EC, 98/34/EC, 2004/22/EC, 2007/23/EC, 2009/23/EC and 2009/105/EC of the European Parliament and of the Council and repealing Council Decision 87/95/EEC and Decision No 1673/2006/EC of the European Parliament and of the Council.

[i.7] 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.8] ETSI TR 103 306: "CYBER; Global Cyber Security Ecosystem".

[i.9] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

NOTE: An update is in progress.

[i.10] ETSI Directives.

[i.11] ETSI TS 103 436: "Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios".

[i.12] ETSI TR 103 935: "Cyber Security (CYBER); Assessment of cyber risk based on products' properties to support market placement".

[i.13] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.14] ETSI TR 103 936: "Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control".

[i.15] ETSI GR SAI 001: "Securing Artificial Intelligence (SAI); AI Threat Ontology".

[i.16] 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.17] ISO 15408-3: "Information security, cybersecurity and privacy protection: Evaluation criteria for IT security. Part 3: Security assurance components".

NOTE: The above document is also available (without ISO cover) from https://www.commoncriteriaportal.org/files/ccfiles/CC2022PART3R1.pdf.

[i.18] ETSI TR 103 937: "Cyber Security (CYBER); Cyber Resiliency and Supply Chain Management".

[i.19] ETSI TR 103 603: "User Group; User Centric Approach; Guidance for providers and standardization makers".

[i.20] ISO/IEC 5962: "Information technology; SPDX® Specification V2.2.1".

[i.21] ISO/IEC 28001: "Security management systems for the supply chain; Best practices for implementing supply chain security, assessments and plans; Requirements and guidance".

[i.22] ISO/IEC 28002: "Security management systems for the supply chain; Development of resilience in the supply chain; Requirements with guidance for use".

[i.23] ETSI TR 103 838: "Cyber Security; Guide to Coordinated Vulnerability Disclosure".

[i.24] ETSI TR 103 305 (all parts): "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence".

[i.25] ISO/IEC 27000: "Information technology; Security techniques; Information security management systems; Overview and vocabulary".

[i.26] IEC 62443: "Industrial communication networks - Network and system".

NOTE: The above reference is to the IEC 62443 series found in 9 standards grouped into 4 parts.

[i.27] ETSI TR 103 395: "Smart Body Area Network (SmartBAN); Measurements and modelling of SmartBAN Radio Frequency (RF) environment".

[i.28] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.29] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.30] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.31] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.32] ETSI ES 202 553: "Methods for Testing and Specification (MTS); TPLan: A notation for expressing Test Purposes".

[i.33] ETSI TS 103 732-1: "CYBER; Consumer Mobile Device; Part 1: Base Protection Profile".

[i.34] ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[i.35] ETSI TS 103 701: "CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements".

[i.36] ETSI TS 103 850: "Reconfigurable Radio Systems (RRS); Definition of Radio Application Package".

[i.37] ETSI GR ZSM 010: "Zero-touch network and Service Management (ZSM); General Security Aspects".

[i.38] ETSI GS ZSM 014: "Zero-touch network and Service Management (ZSM); ZSM security aspects".

[i.39] ISO/IEC 29147: "Information technology; Security techniques; Vulnerability disclosure".

[i.40] ISO/IEC 30111: "Information technology; Security techniques; Vulnerability handling processes".

[i.41] European Union Guide to types of Legislation.

[i.42] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[i.43] Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU.

[i.44] Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166. .

[i.45] ISO/IEC 15408: "Information security, cybersecurity and privacy protection: Evaluation criteria for IT security".

NOTE: The above reference refers to the entire series which is also available (without ISO cover) from https://www.commoncriteriaportal.org/cc/index.cfm.

[i.46] The United States Department of Commerce: "The Minimum Elements For a Software Bill of Materials (SBOM) Pursuant to Executive Order 14028 on Improving the Nation"s Cybersecurity".

[i.47] ETSI TS 103 732-2: "CYBER; Consumer Mobile Device; Part 2: Biometric Authentication Protection Profile Module".

[i.48] ETSI EG 203 367: "Guide to the application of harmonised standards covering articles 3.1b and 3.2 of the Directive 2014/53/EU (RED) to multi-radio and combined radio and non-radio equipment".

[i.49] ETSI TS 103 096 (all parts): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security".

[i.50] ETSI TS 103 732-3: "CYBER; Consumer Mobile Device; Part 3: Multi-user Protection Profile Module".

[i.51] ETSI GS QKD 016: "Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules".

[i.52] ETSI EN 319 403-1: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.53] ETSI TS 103 848 (V1.1.1): "Cyber Security for Home Gateways; Security Requirements as vertical from Consumer Internet of Things".

[i.54] ETSI TS 103 931: "Cyber Security (CYBER); Network Router Security Requirements".

[i.55] ISO/IEC TR 5895:2022: "Cybersecurity; Multi-party coordinated vulnerability disclosure and handling".

[i.56] Recommendation ITU-T X.1250: "Common vulnerabilities and exposures".

[i.57] Recommendation ITU-T X.1055: "Risk management and risk profile guide".

[i.58] Recommendation ITU-T X.1205: "Overview of cybersecurity".

[i.59] Recommendation ITU-T X.1332: "Security guidelines for smart metering service in smart grids".

[i.60] Recommendation ITU-T X.1642: "Guidelines for the operational security of cloud computing".

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
AI	Artificial Intelligence
ANEC	European Association for the Co-ordination of Consumer Representation in Standardization
B2B	Business-to-Business
CC/PP	Common Criteria/Protection Profile
CDMA	Code Division Multiple Access
CIA	Confidentiality Integrity Availability
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CVSS	Common Vulnerability Scoring System
DoC	Declaration of Conformance

DORA	Digital Operational Resilience Act
DoS	Denial of Service
DPIA	Data Privacy Impact Assessment
EAL3	Evaluation Assurance Level 3 (number indicates the level)
EAL4	Evaluation Assurance Level 4 (number indicates the level)
eIDAS	electronic IDentification, Authentication and trust Services
EMC	Electro Magnetic Compatability
ENISA	European Network and Information Security Agency
ESI	Electronic Signatures and Infrastructure

NOTE: ETSI Technical Committee.

ESO	European Standards Organizations
ETI	Encrypted Traffic Integration (ETSI Industry Specification Group)
FDMA	Frequency Division Multiple Access
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
HAS	Harmonised Standard Consultant
hEN	Harmonised European Norme
HF	Human Factors

NOTE: ETSI Technical Committee.

HS	Harmonised Standards

NOTE: The form of an HS is often given as a Harmonised European Norme (hEN).

HSM	Hardware Security Module
IAM	Identity and Address Management
ICT	Information Communication Technologies
IIoT	Industrial IoT
IoT	Internet of Things
IT	Information Technology
ITS	Intelligent Transport Systems

NOTE: ETSI Technical Committee.

NIS2	Network and Information Security (Directive) v2
NIST	National Institute of Standards and Technology
NLF	New Legislative Framework
NVD	National Vulnerability Database
OJ	Official Journal
OJEU	Official Journal of the European Union
OS	Operating System
OSI	Open Systems Interconnection
PDL	Permissioned Distributed Ledger
PKI	Public Key Infrastructure
POSIX	Portable Operating System Interface
PP	Protection Profile
QKD	Quantum Key Distribution

NOTE: ETSI Industry Specification Group.

QSC	Quantum Safe Cryptographiy
QWAC	Qualified Website Authentication Certificate
RRS	Reconfigurable Radio Systems

NOTE: ETSI Technical Committee.

SAI	Securing Artificial Intelligence

NOTE: ETSI Technical Committee.

SAREF	Smart Appliance Reference ontology
SBOM	Software Bill Of Materials

SDO	Standards Development Organizations
SET	Secure Element Technologies

NOTE: ETSI Technical Committee.

SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SPDX®	Software Packet Data Exchange
TB	Technical Body
TC	Technical Committee
TDL	Test Description Language
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TTCN	Testing and Test Control Notation
TVRA	Threat Vulnerability Risk Analysis
VPN	Virtual Private Network
WTO	World Trade Organization
ZSM	Zero-touch network and Service Management

4 Overview of the Cyber Resilience Act

4.1 Core expectations and rationale

The intent of the Cyber Resilience Act (CRA) [i.1] is stated in the explanatory text of the CRA and across the set of recitals, and additionally in the supporting documentation [i.4].

The impact of the CRA is that it will create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. Four specific objectives have been set out:

1) ensure that manufacturers improve the security of products with digital elements since the design and development phase and throughout the whole life cycle;

2) ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;

3) enhance the transparency of security properties of products with digital elements; and

4) enable businesses and consumers to use products with digital elements securely.

The concerns raised by the CRA are summarized in figure 1.

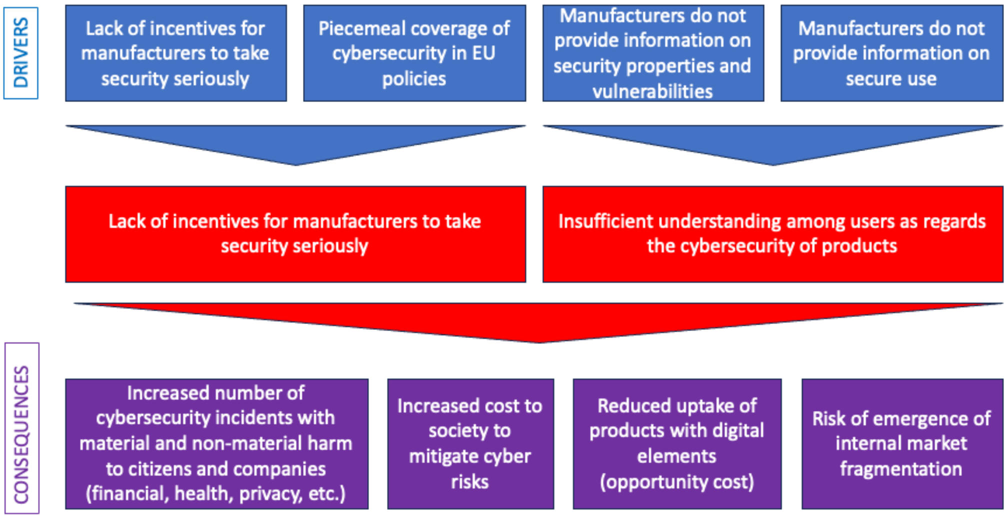
DRIVERS
Lack of incentives for manufacturers to take security seriously
Piecemeal coverage of cybersecurity in EU policies
Manufacturers do not provide information on security properties and vulnerabilities
Manufacturers do not provide information on secure use
Lack of incentives for manufacturers to take security seriously
Insufficient understanding among users as regards the cybersecurity of products
CONSEQUENCES
Increased number of cybersecurity incidents with material and non-material harm to citizens and companies (financial, health, privacy, etc.)
Increased cost to society to mitigate cyber risks
Reduced uptake of products with digital elements (opportunity cost)
Risk of emergence of internal market fragmentation

Figure 1: Concerns addressed in the CRA

The domains of concern are represented by the red boxes leading to the societal concerns in the purple boxes. The CRA seeks to address the items in the blue boxes that will mitigate the concerns of the red boxes and therefore seek to eliminate the societal concerns in the purple boxes.

NOTE 1: The objective is for products with fewer vulnerabilities being placed on the market which appears to accept that it is not possible for vulnerabilities to be completely excised from products.

There is a fair assessment that security is not widely addressed because it has not been addressed in many systems as an essential requirement and the CRA aims to close that gap. At the time of drafting of the proposed CRA, there are no ETSI standards cited by the Official Journal of the European Union (OJEU) that have security as a topic. A manufacturer placing product on the market is aware of radio regulation and safety regulation as gateways to be passed to get to the market. Some regulation, such as GDPR, have focussed attention on the use and application of data, and made the conduct of a Data Privacy Impact Assessment (DPIA) an essential business process, along with the acceptance of having business roles addressing GDPR compliance in organizations. It has been possible to place products on the market that have no cybersecurity protections and the CRA closes that gap with a view to ensuring that due care is taken to identify the risk and to give appropriate protection against any potential exploit.

NOTE 2: The language of the CRA is that cybersecurity protections are provided commensurate to the risk. Therefore it may be possible to place devices on the market without cybersecurity protection as even with a digital element present there may be no means of exploiting that digital element to present a risk to any user. However, it is recognized that due attention should be given to side channel exploits of digital elements where the digital elements that are part of a device or service may be secure but, where their presence can be determined, and exploited, to give rise to risk in an unconnected direction.

The "with digital elements" scope of the CRA is critical. This scope addresses almost all components with electronics, and all components with digital processing or storage. The CRA does appear to bind the coverage of cybersecurity in EU policies but it is noted that many EU regulations address cybersecurity provisions. The present document does not provide any analysis of the content of EU policy.

NOTE 3: Policy and regulation are considered quite distinct for the present document (see https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en [i.41]). Policy is therefore the high level guidance of direction whereas regulations are the means to implement elements of the policy. Thus a policy may be to "ensure the citizens of the EU are protected from cyber attack" and the regulations, directives, and acts, such as CRA [i.1], CSA [i.3] and NIS2 [i.2] enable the policy to be implemented.

The CRA [i.1] introduces the notion of "non-tangible product", i.e. software is considered as a product under the CRA legislation, which also introduces ambiguity about whether remote services associated with a product (tangible or not) may be considered in scope. While the CRA intends to rely on the New Legislative Framework (NLF) [i.5], the current version of the NLF does not cater for a "non-tangible products" category.

It is also recognized that the CRA requirements intend to cover the entire lifecycle of a device, while the scope of the NLF is centred exclusively on products at the time they are placed on the market. This may introduce some ambiguity with regards to the legislation applicable to a manufacturer where standards may support one but not the other. The CRA has in its scope a manufacturer's development lifecycle processes, such as vulnerability disclosure, but also device specific lifecycle phases that take place post market placement, including support of multiple configuration and provisioning phases of an IoT product during its operation. Typically, these later phases happen under the responsibility of a diversity of stakeholders who are likely to be independent of, and in many cases unknown to, the product manufacturer.

NOTE 4: Post market placement stakeholders identified in the CRA include system integrators, network operators, facility owners, maintenance operators.

This complexity would have been reduced if the CRA scope had been restricted to the Consumer market only, but the legislation as proposed applies indifferently to Business-to-Business (B2B) products, which have to accommodate potentially complex vertical ecosystems and deployment considerations, especially in the IoT field. In particular, B2B IoT devices are often integrated for specific purposes based on Business Agreements involving processing elements, sensors and actuators, connectivity stack and applicative software, so that manufacturer's liability tends to be split among multiple actors depending on business agreements.

One key point that appears throughout the CRA is the process of "secure by default" which raises a timing issue. It has been the contention of security engineers for all time that security cannot be an add-on. This applies equally to safety engineering - it cannot be added after the fact. Security mechanisms cannot be seen as discrete components to be switched on or off at random. This means that the tools for design and implementation have themselves to be (cyber)security aware and trap errors, including those of absence, early in the design phase. For the CRA this requires acceptance of products or services having "digital elements" and building CRA compliance/conformance into products and services from the beginning.

The subject matter of the NIS2 Directive [i.2] (Article 1) states "*... lays down measures that aim to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market*" where the same text in the CRA states "*... rules for the placing on the market of products with digital elements to ensure the cybersecurity of such products*", and the CSA [i.3] states in its own Article 1 "*... with a view to ensuring the proper functioning of the internal market while aiming at a high level of cybersecurity, cyber resilience and trust … lays down a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products, processes and services*". It can be reasonably stated that the 3 are complimentary in that they all aim to achieve a high level of cybersecurity where the CSA specifically addresses certification schemes and assurance with the NIS2 addressing certain forms of economic operator. It would be a reasonable expectation that a small set of standards form a common core of capabilities across multiple regulations.

NOTE 5: There are exceptions to the CRA for some markets (see clause 4.4) but such exceptions are only contingent on the exempted markets meeting the same expectations as the CRA.

NOTE 6: The CRA is noted to have some overlap with the requirements of the Digital Operational Resilience Act (DORA) where cybersecurity requirements and digital elements appear in the financial market.

NOTE 7: There are some national initiatives that may also be impacted by the CRA including the UK's Code of Practice for apps and app-stores where an app may be fairly characterized as a digital element (i.e. there is a risk that national codes of practice may be sidelined by strict conformance to the CRA or that they be updated to encompass the CRA).

4.2 Role of standards and SDOs

Standards as published by Standards Development Organizations (SDOs) and the subset of SDOs that have special status in Europe as European Standards Organizations (ESOs) - made up of CEN, CENELEC and ETSI - are considered voluntary. In some circumstances specific standards may be cited by regulation and conformance is required to place products covered by those standards on the market.

NOTE 1: Many bodies develop standards and take the honorific title of Standards Development Organizations and an overview of the eco-system around security standards and technology can be found in ETSI TR 103 306 [i.8].

It is useful to understand what is meant by an international standard. In this context there is a formal definition and what may be considered as a layman consideration. Formal definitions for the EU can be found in Regulation (EU) No 1025/2012 [i.6] where "international standard" means a standard adopted by an international standardization body, and that is further defined in Article 2, point (9) as meaning the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). This formal definition is somewhat at odds with the eco-system for standards development and with the various internationally recognized standards from IEEE, ETSI, IETF and many others. However, it is noted that Regulation (EU) No 1025/2012 states that the ESOs are founded on principles approved by the World Trade Organization (WTO) of coherence, transparency, openness, consensus, voluntary application, independence from special interests, and efficiency. It should be reasonable to assert that any SDO abiding by these principles is an appropriate source of international standards. It is strongly asserted that ETSI conforms to the principles of the WTO. In addition, it is also noted that there are three formally recognized European Standards Organizations (CEN, CENELEC and ETSI) by Annex I of Regulation 1025/2012.

NOTE 2: The definition of European standards versus International standards is addressed in the definitions section (Article 2) of Regulation 1025/2012 [i.6] and only refers to the body publishing the standard and not to geographic relevance.

It can be argued that some Industrial sectors are more or less open to the role of standards, and the purpose of standards with respect to market access is viewed differently in some sectors than in others. The telecommunications industry, and the domestic power market (as examples), have been dependent on standards for interoperability for many years and this commitment to interoperability standards has fed into safety and security standards too. In short, safe and secure are essential components of interoperability. In some industrial sectors interoperability is less of an issue (one toy from one vendor does not have to interoperate with toys from another vendor) and the culture of standards is perhaps less dominant in such environments. However, the connected world, where there is increasing interconnectedness of devices that need to address security, safety and interoperability is extended to many more industries. If there is no culture of such standards, and of the design requirements they impose, there is a significant chance of exactly the concerns addressed by the CRA.

Not all of the industries developing interconnected devices have been exposed to the role of SDOs or of standards to an equal extent. The leading SDOs view the standards they produce as challenging to conform to, but by being challenging the SDOs assert that they raise the bar, particularly in security and safety. In addition, SDOs review and update standards to make sure that the safety or security they offer to products is maintained over time. This is particularly important for security where the capabilities of attackers evolve, and improves, requiring similar evolution and improvement in the capabilities of the standards.

NOTE 3: The role of vulnerability awareness and reporting extends to SDOs too and at ETSI this is addressed in ETSI's Coordinated Vulnerability Disclosure process. This is available at https://www.etsi.org/standards/coordinated-vulnerability-disclosure.

4.3 The security standards environment

4.3.1 Addressing the attack surface

Security measures in general seek to minimize the attack surface of a system. Many of the core principles of strategies such as "secure by design", "secure by default", "zero trust" and so on, seek to both illuminate and minimize the attack surface. The role of attack surface illumination is to make it clear to the developer where an attacker is able to exploit the system and does so by making clear where there are interfaces or ports that an attacker can use to access the system. Once the attack surface is known the developer is able to make steps to minimize the likelihood of an attack by maximizing the defence of the attack surface, with the effect of minimizing the exploitable attack surface.

There is some ambiguity in the language surrounding vulnerability. The approach used in ETSI's TVRA (ETSI TS 102 165-1 [i.9]) is that all systems have weaknesses, and those weaknesses become vulnerabilities when an exploit of them exists. The approach taken in the TVRA is to determine the risk of exploit, the mechanism of exploit, and to identify measures that mitigate against exploit of the weakness (i.e. to mask or remove the weakness in such a way that the weakness is not open to exploit).

NOTE: When developed, the intent of the TVRA was to be used as a means to provide a detailed rationale for the development of standards. The current use and application of TVRA is wider than just as a rationale for standards work but addresses the wider rationale for the application of countermeasures to threats and threat agents across any cyber domain. The continuous update programme of the TVRA approach to address new contexts, including that of the CRA, is intended to ensure that approach remains applicable.

Even a minimal attack surface may be exploitable by its vulnerability profile. Although all attack surfaces have weaknesses not all of those weaknesses are immediately, or ever, exploitable by the attacker. It is also recognized that sharing knowledge of a potential vulnerability before there is a means to protect against its exploit may lead to an exploit being developed and an attack launched. This requires a reasonable balance between sharing developer knowledge of their risk assessed attack surface, and giving a developer time to patch or otherwise protect against exploit of the attack surface. At the same time, developers should be able to access reasonable knowledge of similar vulnerabilities to maintain the goal of attack surface minimization. The role of vulnerability disclosure in this attack surface management domain and the risk of over sharing knowledge of an attack surface includes minimization of the attack surface by minimization of dissemination through vulnerability disclosure reports.

4.3.2 Modal verbs, mandates and recommendations

ETSI's working processes are fully specified in ETSI Directives [i.10] and a simplified view of them is given here. ETSI, like most SDOs, prepares a wide range of technical material. In principle there are two broad classes of material:

1) Reports.

2) Specifications.

ETSI reports are intended to give advice on a technical topic and are not intended to be directly implemented, tested and used in a way that is considered to be binding. However, reports are often very strongly advisory and may serve as the basis of codes of practice or similar best practice statements. The only significant distinguishing element between the forms of report produced by ETSI (TRs → Technical Reports, EGs → ETSI Guides, GRs → Group Reports, SRs → Special Reports) is the means by which they are approved for publication. A recommendation in a report is signified by the modal verb should. It is also recognized that reports are often used as a precursor to a more detailed technical requirement or, as is the case in groups such as ISG SAI and in ISG QSC (before its absorption into TC CYBER as a Working Group), to highlight a particular threat or opportunity and to map out the necessary requirements to be developed.

The second major class of documents prepared are those that set out normative requirements that can be implemented and tested to ensure that the implementation conforms. Such documents are called Specifications or Normes, the only ones from ETSI that are allowed to use the modal verb "shall". Again, like for reports, there are a range of document labels applied to requirements documents where the significant distinguishing element is the means by which they are approved for publication (ENs and HSs → (harmonised) European Normes, ES → ETSI Specification, TS → Technical Specification, GS → Group Specification).

In the day-to-day working practice across most SDOs the intention is to achieve consensus. Mechanisms do exist for voting, and voting is applied for ENs by the National Standards Organizations in the ETSI EN Approval Process (ENAP) and for Standardization Request deliverables Approval Process by the National Standards Bodies. Where voting is applied in ETSI Technical Bodies it is conducted strictly in accordance with ETSI's Directives.

4.3.3 Technical measures

In relatively simple terms technical security measures support the paradigm of Confidentiality Integrity Availability (CIA) in order to provide assurances of each of Confidentiality, Integrity and Availability of services. There are many ways of achieving each of these attributes where the environment in which services, devices and applications will be deployed are widely varied:

- Confidentiality - to ensure that data shared by PartyA with PartyB cannot be seen by an adversary, PartyC.
- Integrity - to ensure that data shared by PartyA with PartyB is only that data shared and that it has not been manipulated by an adversary, PartyC.
- Availability - to ensure that data intended for PartyA is only available to PartyA when PartyA needs it.

A more comprehensive analysis of the mapping of technical measures to the CRA is provided in clause 6 of the present document. However in summary there are a number of approaches to be taken at a technical level that support a general requirement of ensuring that the system operates to principles of least privilege and least persistence. The least privilege principle requires that data is only made available to those who really need that data, and everyone else is excluded. The least persistence principle is slightly less obvious but essentially is to ensure that security relationships expire as soon as is practical at a cost in re-verification (i.e. there is a trade-off between the cost of verification and the cost or risk of retaining a relationship (e.g. using cookies in web-browsers may reduce verification cost but requires the cookie is protected)).

It is noted that ETSI has made a substantial start in addressing some of the more nuanced issues of societal security in standards, in particular addressing the coercive use of IoT technologies. This is addressed in the development of ETSI TR 103 936 [i.14] with a scope of addressing both Coercive control resistant design and Trauma informed design.

4.3.4 Risk assessment and analysis standards

The technical model of risk assessment is summarized in the following diagram taken from ETSI TS 102 165-1 [i.9] (see figure 2).

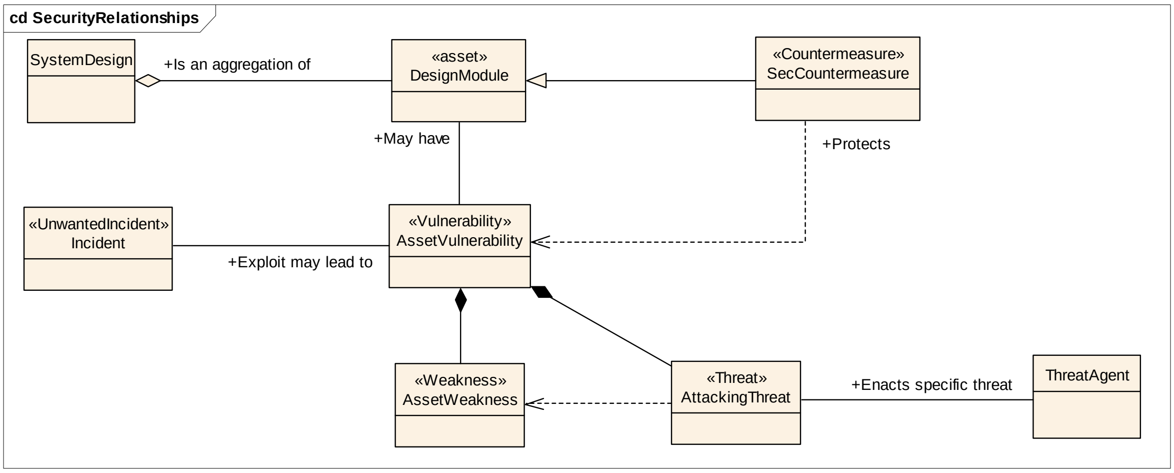

Figure 2: Technical model of risk assessment from ETSI TS 102 165-1 [i.9]

This can be summarized in text as: A system consists of assets (an aggregation of assets). An asset may be physical, human or logical. **Assets** in the model may have **Weaknesses** that may be attacked by **Threats**. A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking certain pre-defined security objectives. A **Vulnerability** is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**. When applied, **Countermeasures** protect against **Threats** to **Vulnerabilities** and reduce the **Risk.**

Risk is further considered in the technical domain as being the product of the impact of an attack on the asset, and the likelihood of that attack.

It is noted of course that risk is much more than simply about identifying technical countermeasures and much of the available risk analysis and risk management standards that exist do so for non-technical topics. Thus, in ETSI GR SAI 001 [i.15] the business context is addressed when assessing risk as below. Business-centric assessments of risk often overlap with the ICT modelling of risk, although the overall view of risk is focussed on aspects of business continuity and address a slightly different set of indicators than for the ICT modelling shown in ETSI TS 102 165-1 [i.9] (see figure 2).

Table 1: Business assessment indicators for risk modelling

Indicator	Risk assessment questions
Magnitude	What risks will failure create? Classifications of where risk lies include: • Monetary loss (i.e. direct financial impact) • Compliance (i.e. will existing compliance procedures be maintained) • Legal (e.g. will existing legal safeguards apply) • Reputation (e.g. how will readiness or failure to be ready impact the reputation of the organization either in absolute terms or by comparison to peer and competitor organizations)
Duration	How long has operation to be maintained for each asset or class of assets impacted?
Scope	How far down the supply chain is the impact to be addressed?
Severity	Can damage due to degradation or interruption of each service be quantified?
Response	Is there a plan to migrate compromised components to alternative modes of operation?

In updating ETSI's TVRA method some of the analysis and text from the business and non-technical domain will be addressed.

Across ETSI there are a number of groups that address security concerns from a user perspective, including TC HF, TC USER, and ETSI's close relationship to ANEC and other bodies through the mechanisms of the ETSI Board Strategy Group on Inclusiveness (BOARD INCLU). See also clause 4.3.5.

4.3.5 Societal security standards

Any discussion of societal security almost always overlaps with societal safety. The various tools of cybersecurity protection mitigate against cyber-attack, but if an attack is made the result can be loss of data or similar (see the attack tree below). In preventing attacks there are many additional levels of protection that include many non-technical barriers. Such non-technical barriers include the act of ensuring that cyberattacks are prosecuted in similar manner to a physical attack. There are barriers to overcome in this. In the cyberworld the form of attack and exploit has taken new forms and the tools to exploit are widely distributed. There is therefore a race between a capability being offered for a "good" purpose and that same capability being used for a "bad" purpose.

Effort is being made in ETSI already in trying to address some of these concerns, e.g. the work item in ETSI CYBER on coercive behaviour to be published as ETSI TR 103 936 [i.14].

EXAMPLE 1: Theft of a physical object denies the correct owner from using the physical object (e.g. if a car is stolen the legitimate owner does not have that car to use any more), but stealing a cyber object may mean making a duplicate that is used by the thief whilst the correct owner retains full use of the cyber object.

EXAMPLE 2: AI can generate entirely fake images (e.g. using forms of generative AI or text-to-image generators) that invoke harm on a subject but where conventional CIA cybersecurity paradigms may not be able to counter the attack or harm (initial generative AI has been seen to produce image artefacts for example that would not appear in a "real" image although it is likely that this will be less likely over time). It is noted however that such technology is also used in the entertainment industry to place an actor in a fake environment intentionally without intent to cause harm.

EXAMPLE 3: A remote heating controller is intended to give confidence that a homeowner or tenant can ensure heating is on or off when they are not in the home, however, that same facility can be used to deny heating to tenants or overheat a home as a psychological attack on the tenants.

It is recognized that having accountability for the provider of AI services is one of the mitigations of these AI based risks, and this could be provided through QWACs or QSeal Certificates (see also clause 8).

It is also recognized that cybersecurity has a different meaning to different stakeholders. If a product or service is offered by some combination of electronics, software and communications technology (ICT in general) then any attack delivered by that ICT technology is perceived as a cyberattack and therefore should be addressed by cyber-security. The consequence of this is that content based attacks, e.g. AI generated deep fakes, are considered as cyberattacks, and manipulation may be seen only in content, even where that content passes the conventional CIA protections. Similarly attacks that use software to manipulate data or software, e.g. viruses and trojans, are cyberattacks. Cyber defence therefore not only addresses the CIA paradigm (see clause 6 of the present document) but also content and intent to mitigate and prevent harm.

EXAMPLE 4: Internet memes often use fakery in their creation and whilst often intended to poke fun at the subject may also be considered as attacks on the subject. If AI can make the meme more convincing and increase the damage it may be viewed as a cyber security risk.

4.4 Scope of impact of CRA

The following set of stakeholders are noted in the Impact Assessment Report as being mainly affected by the CRA:

- Software manufacturers
- Hardware manufacturers
- Importers of products with digital elements
- Distributers of products with digital elements
- End-users, including businesses, public authorities and consumers
- Market surveillance authorities
- Accreditation and notifying authorities

- Notified bodies

Successful standardization therefore should involve all of these stakeholders in order to be able to collectively address the underlying drivers that have prompted the CRA (the blue boxes) and led to the concerns the CRA identifies (the red boxes) in order to prevent the effects on society outlined by the CRA (the purple boxes).

It is recognized that there are some exceptions to the CRA (Article 2) that are managed by different regulatory frameworks:

- Medical devices (as defined in article 2 of Regulation (EU) 2017/745 [i.42]).
- In-vitro medical devices (as defined in article 2 of Regulation (EU) 2017/746 [i.43]).
- Vehicles subject to type approval in categories M, N and O (as defined in Regulation (EU) 2019/2144 [i.44]).

In making sense of the CRA due consideration should be given to the possibility of misunderstanding of its role, particularly with respect to the NIS2 and CSA regulatory frameworks where there is some overlap and mutual dependency.

ETSI Standards are generally proposed by members in reaction to a perceived shared concern. Whilst the present document identifies several aspects of ETSI's output that map to core requirements cited in the CRA the model most often applied in ETSI is not to create standards for specific regulation, rather the regulatory context is treated as an environmental factor that assists in forming the standard's content. Thus, as also stated in clause A.2, a single standard may address many points of regulation, or in some cases a regulation may be cumulatively addressed by a combination of several standards.

NOTE: There are also cases where the EC requests ETSI to draft Harmonised Standards or European Standardization Deliverables in support of European regulation (which can only be developed in response to an EC request). More information on this case can be found at ETSI - Supporting regulation & legislation, harmonised standards, ESO.

4.5 Standards and Certification

Regulation (EU) 2019/1020 [i.7] of the European Parliament and of the Council (regarding market surveillance) apply to products with digital elements covered by the CRA. The expectation is that each product will have a "Declaration of Conformity" (DoC) that identifies all the essential requirements that stem from the various legal acts that apply to the product that the product conforms to. The expectation is that the essential requirements will be specified in technical terms in Harmonised Standards cited in the Official Journal (OJ) against specific regulation.

Conformance to a harmonised standards that have been cite in the OJ (Article 18) gives presumption of conformity with the essential requirements of the legislation. During HAS consultant assessment there is a risk that the assessment of the standard may uncover vulnerabilities that have been developed between completion of the technical content and the HAS assessment (see also the note below). The speed at which a standard can be updated to address a fault is important to consider and the requirement to implement a vulnerability disclosure and reporting process (in Annex I, clause 2 of the CRA) and to fix faults should also be applied to the standardization element of products and services subject to the CRA.

NOTE 1: Most (but not all) product vulnerabilities are unrelated to the standards but result from implementation weaknesses that do not affect compliance to the implemented technical standards.

If a vulnerability exists that is a direct consequence of a specific standard it should be fixed. In this specific regard ETSI operates a vulnerability reporting programme with a view to ensuring that if the standard itself contributes to a vulnerability that it can be assessed and fixed:

LINK: https://www.etsi.org/standards/coordinated-vulnerability-disclosure#:~:text=When%20submitting%20a%20vulnerability%20report,enable%20reproduction%20of%20the%20vulnerability.

A summary of the status of ETSI's output of Harmonised standards is that 183 Harmonised standards from ETSI have been cited in the OJ (158 related to RED, 3 to EMC, 1 for accessibility). None of these HSs appear to have any keywords from the security set and there are an additional 75 HSs that are not cited in the OJ. The non-existence of security standards in the OJ should not be a concern as the OJ has direct legislative role and often implies that the cited standards were produced by an EU accredited ESO under a Standardization Request in support of Essential Requirements under the NLF. If such SRs have not been raised it would be unlikely that standards are cited in the OJ. This should not be interpreted that security standards do not exist. They do and the present document attests to their value in meeting the objectives of the CRA.

EXAMPLE: Whilst SDO published standards exist for computer operating systems most are de-facto from very large IT companies and do not cite any requirements or conformance to SDO standards (with the exception of framework standards such as POSIX (allowing for software portability between operating systems)).

An EN (or HS) may be developed by an ESO in response to a specific Standardization Request (SR) from the European Commission in relation to essential requirements of a regulation. The EN (or HS) which is then cited in the OJ, infers that an implementation of the standard is granted "presumption of conformity" with the essential requirements of the underlying legislation. This has the meaning that a simple declaration by a manufacturer that they have implemented and are compliant with the standards is sufficient to be deemed in conformity with the essential requirements. Application of such standards remains optional. Manufacturers may choose to conform to the essential requirements in some other way and would be expected to demonstrate conformity against the essential requirements of the legislation by having their product assessed by a third party Notified Body.

However, the presumption of conformity may not be granted only on the basis of a manufacturer's self-declaration, and in some cases specific 3rd party testing will be required to be undertaken by recognized test houses (Notified Bodies). In the security domain this is addressed in part by the provisions of the CSA and the role of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products, processes and services. The expectation of when to apply such certification schemes, in addition to the CRA, is identified in the classification of risk in the CSA and the required assurance level (basic, substantial, high).

NOTE 2: Self-conformity declarations under the CSA are only allowed in very specific circumstances and generally, but not exclusively, apply to low-risk products and services.

NOTE 3: When mapping to assurance schemes such as Common Criteria there is a rough mapping of substantial to EAL3 and of high to EAL4+.

Decision No 768/2008/EC [i.16] of the European Parliament and of the Council establishes modules for conformity assessment procedures to essential requirements set by EU legislation in proportion to the level of risk involved and the level of security required.

To quote from the requirement in Annex I. 1.3 products with digital elements (quote) "…***shall be delivered with a secure by default configuration, including the possibility to reset the product to its original state;***".

The manufacturer may be able to attest to the secure by default configuration - in this state this attestation can be verified by a 3rd party. The question here is how is this default configuration state tested?

The manufacturer attests that if the product with digital elements evolves away from its default configuration that it can be reset to its prior state. However, the prior state may no longer be secure (as the attacker evolves). Lifetime revision of the DoC of a product has been addressed in TC RRS (see ETSI TS 103 436 [i.11]) in which a new declaration of conformity can be delivered to the device. This approach has shown that mechanisms exist to address the mutability of devices where new states (e.g. OS updates) still achieve the objective of being secure by default.

In summary ETSI has taken steps across its standards development process to ensure that a staged approach is followed where the final stage is some form of proof of conformance to the standard and this is applied equally in the security standards domain. However, it is noted that depending on Assurance Level, security assessment may go well beyond proving compliance with requirements from a standard, whatever the underlying standard, and even the most stringent security certification can never provide certainty about security, which remains influenced by subjective factors related to risk assessment and acceptance.

NOTE 4: There may be many ways in which proof of conformance can be given including the results from the application of a formal test suite, and detailed expert evaluation of the implementation against strict evaluation criteria.

5 Mapping of standards to requirements extracted from CRA articles

5.1 Mapping for Article 10

Article 10.2a of the original proposal of the CRA states: "*When placing a product with digital elements on the market, the manufacturer shall include a cybersecurity risk assessment in the technical documentation as set out in Article 23 and Annex V*".

The corresponding text in Article 23 states:

- *"The technical documentation shall contain all relevant data or details of the means used by the manufacturer to ensure that the product with digital elements and the processes put in place by the manufacturer comply with the essential requirements set out in Annex I. It shall at least contain the elements set out in Annex V".*

The corresponding text in Annex V states:

- *"An assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation".*

There is a small set of standards that identify how to document and carry out a cybersecurity risk analysis and a fairly small set that document the actual risk analysis taken for any particular subject matter. There is some further uncertainty in this respect where the approach to risk is determined (e.g. is the almost wholly technical analysis of ETSI TS 102 165-1 [i.9] appropriate, or is a wider business risk analysis also expected?). It is noted that the CSA approach is based on application of the AVA_VAN class from ISO 15408-3 [i.17] which is not straightforward to apply to a technical standard but for which some guidance is being considered in ETSI's TC CYBER as a new subpart of ETSI TS 102 165 (expected to be published as ETSI TS 102 165-3 when completed).

NOTE 1: The active work item intended to give guidance to the application of the AVA_VAN class in a technical risk analysis environment is seen here https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=69133.

In recognizing that there is a gap in the guidance available to manufacturers from ETSI on how to conduct and document a risk analysis with respect to the expectation of the CRA it has been proposed to extend the TVRA method with an extension for AVA_VAN. This should then be further developed to prepare a normative framework for the documentation elements that address risk assessment and mitigations as outlined for Article 10.

It is noted that the approach of each of Common Criteria (cited in ETSI work and published as ISO/IEC 15408 [i.45]) and in ETSI TS 102 165-1 [i.9] is technical and identifies risk of an attack occurring from an analysis of the impact of the attack and the likelihood of the attack. However, in many other domains, including the CRA, the role of likelihood of the attack is often suppressed and risk is rather considered by the form of asset or stakeholder that is impacted.

EXAMPLE 1: Where the primary stakeholder is a child (minor) the risk is often stated as high by default almost irrespective of the likelihood of an attack, as the impact is to a child and child protection takes precedence over assessment of likelihood.

EXAMPLE 2: Where the primary asset is private data the risk if often stated as high by default, where the intent is to ensure that irrespective of the likelihood of attack to the private data that such assets are given an assurance of protection in the system design (see also the penalties for failing to do under GDPR).

In recognizing that different interpretations of risk are possible it is further strongly recommended that such factors (stakeholder or asset type with special characteristics) are taken into more account in the framework standards for risk assessment (e.g. in updating ETSI TS 102 165-1 [i.9]). The risk calculation of ETSI TS 102 165-1 [i.9], in common with many other methods of risk analysis, considers both the impact of attack and the likelihood of an attack. The weighting of impact needs care, and sufficient guidance should be given to the analyst to prevent underestimation of actual and perceived impact. This is one of the areas that is subject to review across ETSI in recognizing the widening attack surface that is enabled by ubiquitous connectivity, and the need to assess more nuanced impacts on different user types.

Recital 37 and Article 10.15 of the proposal for the CRA address the supply chain and cite the use of Software Bill Of Materials (SBOM) as a tool in documenting the supply chain, and further cites this in Annex I, section 2.1. ETSI's work item that will lead to the publication of ETSI TR 103 937 [i.18] does address the supply chain as noted in the scope of the work item "*addresses cyber resiliency throughout the supply chain and the various related frameworks and measures using risk-based, system of trust, and zero trust approaches*" and cites the CRA as a major source. In addition, the work in ETSI's ISG ETI on the role of zero-trust approaches in the building of dynamic connections addresses in some detail capabilities that reinforce the supply chain security requirements.

NOTE 2: The definition of software bill of materials given in Article 3 means a formal record containing details and supply chain relationships of components included in the software elements of a product with digital elements.

Thus whilst ETSI has no published standards at the time of writing addressing SBOMs it is clear that an SBOM may be used in implementation of the recommendations from ETSI TR 103 937 [i.18] and addressing the explicability requirements identified by the work of ISG ETI. It is also recognized that there is some activity in other SDOs and government organizations. E.g. https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf [i.46]. It is noted the ETSI USER group has proposed the ACIFO model (Architecture, Communication, Information, Functionality, Organization) in ETSI TR 103 603 [i.19] which addresses supply chain issues from a user centric perspective. In the international standards domain there are a number of candidate standards for SBOMs that may be adopted by reference to the EU as ENs, these include the CycloneDX format and SPDX, available as ISO/IEC 5962 [i.20].

NOTE 3: Whilst the scope of the present document primarily addresses ETSI's standards catalogue it is acknowledged that CEN and ISO have been active in the domain of supply chains and that ISO/IEC 28001 [i.21] and ISO/IEC 28002 [i.22] may apply in this domain.

NOTE 4: In addition it is acknowledged that ENISA has undertaken and published a number of studies and made recommendations for supply chain security. Whilst the ENISA reports are not standards they have been used to direct some of the activity in the SDOs.

The wider content of Article 10 also ties into the content of Article 23 and Annex V with respect to the documentation required for CRA conformance.

5.2 Other articles

5.3.1 Article 23 - Technical Documentation

ETSI does not produce many standards that directly fit to the provision of technical product documentation. However as noted above for risk analysis the ETSI TVRA method does include a pro-forma that can be used in documentation, similarly many of the test domain standards from ETSI include a pro-forma for the provision of test results. Article 23 points to Annex V of the proposal for the CRA where it is clearly indicated what technical documentation has to include:

"1) a general description of the product with digital elements, including:

- *a) its intended purpose;*
- *b) versions of software affecting compliance with essential requirements;*
- *c) where the product with digital elements is a hardware product, photographs or illustrations showing external features, marking and internal layout;*
- *d) user information and instructions as set out in Annex II.*

2) a description of the design, development and production of the product and vulnerability handling processes, including:

- *a) complete information on the design and development of the product with digital elements, including, where applicable, drawings and schemes and/or a description of the system architecture explaining how software components build on or feed into each other and integrate into the overall processing;*

b) *complete information and specifications of the vulnerability handling processes put in place by the manufacturer, including the software bill of materials, the coordinated vulnerability disclosure policy, evidence of the provision of a contact address for the reporting of the vulnerabilities and a description of the technical solutions chosen for the secure distribution of updates;*

c) *complete information and specifications of the production and monitoring processes of the product with digital elements and the validation of these processes.*

3) *an assessment of the cybersecurity risks against which the product with digital elements is designed, developed, produced, delivered and maintained as laid down in Article 10 of this Regulation including how the essential requirements set out in Annex I, Section 1, are applicable;*

4) *a list of the harmonised standards applied in full or in part the references of which have been published in the Official Journal of the European Union, common specifications as set out in Article 19 of this Regulation or cybersecurity certification schemes under Regulation (EU) 2019/881 pursuant to Article 18(3), and, where those harmonised standards, common specifications or cybersecurity certification schemes have not been applied, descriptions of the solutions adopted to meet the essential requirements set out in Sections 1 and 2 of Annex I, including a list of other relevant technical specifications applied. In the event of partly applied harmonised standards, common specifications or cybersecurity certifications, the technical documentation shall specify the parts which have been applied;*

5) *reports of the tests carried out to verify the conformity of the product and of the vulnerability handling processes with the applicable essential requirements as set out in Sections 1 and 2 of Annex I;*

6) *a copy of the EU declaration of conformity;*

7) *where applicable, the software bill of materials as defined in Article 3, point (36), further to a reasoned request from a market surveillance authority provided that it is necessary in order for this authority to be able to check compliance with the essential requirements set out in Annex I."*

In response to each of these there are some applicable ETSI publications, although in all cases the mapping to the explicit requirements is not sufficient for them to be used as the only document set. Rather, as for the pro-forma elements of the TVRA, (P)ICS and test documents, ETSI documents can be used as elements of the document suite.

For Annex V.2.b, the guide to vulnerability disclosure in ETSI TR 103 838 [i.23] then applies as a framework standard. Parts of ETSI TR 103 838 [i.23] could be updated to make certain elements mandatory (as this appears to be the intention of Annex V.2.b).

The risk assessment part of the technical documentation is addressed above for Article 10.

The results of tests as outlined in Annex V.5 where those tests are defined by ETSI, particularly for the TTCN based automated test suites, result in a consistent document identifying all of the marked elements. Furthermore where those test specifications are cited in the OJ they also form part of the documentation suite required by Annex V.4 and Annex V.6.

RECOMMENDATION#1: The documentary support to show how a stakeholder conforms to the CRA is extensive and an ETSI Technical Report that gives a proforma or a checklist for CRA documentation suites should be developed.

5.3.2 Article 5 - Requirements for products with digital elements

All of the essential requirements are outlined in Annex 1, Section 1. The content of Annex 1, Section 1 of the proposal for the CRA [i.1] is copied below with a very short summary to identify if standards exist. A more comprehensive analysis of security standards and the capabilities they encompass is given in clause 6 of the present document.

The CRA requires that "*products with digital elements shall be designed, developed, and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks*, and at the same time *products with digital elements shall be delivered without any known exploitable vulnerabilities"*. The 2 statements may be contradictory - even if there is a theoretically exploitable vulnerability it may actually not impact the risk to the product, hence it would be reasonable to market something with a known vulnerability as the risk of the exploit is insignificant, or the exploit is only theoretical, or where the exploit requires a significant alignment of factors in order to be exploited. An associated concern is that whilst many exploitable vulnerabilities are listed on widely available vulnerability catalogues and the CVSS it is not clear that this can apply in general. The NVD (hosted by NIST) lists 2 950 for December 2022 alone, many for very specific products. There is further uncertainty about the metric that is then used for assessing that the product has been placed on the market *without any known exploitable vulnerabilities* that should be clearly cited.

NOTE: It is also recognized that if there are several thousand entries added to vulnerability catalogues every month that it may not be cost effective or reasonable to expect a developer to verify immunity to any known one.

RECOMMENDATION#2: Definitions that clearly distinguish between known vulnerabilities, and exploitable vulnerabilities, are made available.

Table 2: Mapping of ETSI standards work to essential requirements of the CRA [i.1]

Requirement in Annex I. 1.3	Standards that may apply
Products with digital elements shall …	Based on risk analysis, e.g. ETSI TS 102 165-1 [i.9], or on the application of security controls such as those found in the ETSI TR 103 305 [i.24] series, and elements of each of the ISO/IEC 27000 [i.25] series and IEC 62443 [i.26] series. In addition, the content of ETSI TR 103 395 [i.27] applies.
Be delivered with a secure by default configuration, including the possibility to reset the product to its original state;	ETSI TR 103 309 [i.28]. ETSI EN 303 645 [i.29]. It is noted that the TR giving guidance to the secure by default paradigm should be updated to address normative elements but it is also clear that the EN addresses secure by default too.
Ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems;	Framework in ETSI TS 102 165-2 [i.30] plus many others.
Protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms;	ETSI provides many standards for specific areas of telecommunication where data on exposed interfaces are protected by confidentiality mechanisms including encryption. ETSI also endorses and incorporates standards from other SDOs (e.g. IETF) that enable this, e.g. TLS, IPsec.
Protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorized by the user, as well as report on corruptions;	Mechanisms and standards cited in clause 6.3 apply in a similar way as described above for protection of confidentiality. Similarly ETSI endorses and incorporates standards from other SDOs and like bodies (e.g. NIST's FIPS) that enable this (e.g. SHA).
Process only data, personal or other, that are adequate, relevant and limited to what is necessary in relation to the intended use of the product ('minimization of data');	ETSI's standards are built on a set of principles of least privilege, least persistence and secure by default/design. In adopting such an approach data minimization has become the default. It is noted that many of the public concerns related to this topic are in the content domain and not easily enforced by those standards developed in ETSI that enable operation, interoperability and interconnectivity of products and services.
Protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks;	An analysis and framework for such mitigations is available in the framework document ETSI TS 102 165-2 [i.30]. In addition many of the core radio networking standards and network management standards have provisions to monitor and configure networks in order to mitigate against DoS attacks. It is further noted that core networks, particularly when part of national critical infrastructures, enable such capabilities by default and are subject to various forms of stress testing to verify they are able to mitigate such attacks.

Requirement in Annex I. 1.3	Standards that may apply
Minimize their own negative impact on the availability of services provided by other devices or networks;	A core aspect of the staged approach used in ETSI and other bodies is to identify how any technical provision impacts any other provision, technical or procedural. The guiding principle is to have zero or positive impact on any other services. It should be noted that if a service is used without any security service that when such services are added it may impact the performance a little (authentication and key agreements take time) but that is offset by greater assurance that the service is protected.
Be designed, developed and produced to limit attack surfaces, including external interfaces;	ETSI identifies the vulnerable exposed interfaces and defines measures that protect against exploit through those interfaces. As an SDO ETSI is only able to protect those interfaces that are standardized and essential to the operation of the product or service.

5.3.3 Article 6 - Critical products with digital elements

The identification of critical products meets some of the concerns identified in the analysis against article 10 wherein the risk assessment has to be able to clearly identify a critical product. It is assumed that Article 5 always applies and Article 6 merely extends it.

6 Functional capability standards

6.1 Technical security design paradigms

Much of the technical security work in ETSI standards has been developed to counter specific threats. This is captured in the threat tree from ETSI TS 102 165-1 [i.9] (see figure 3) and in the mapping from that to the Confidentiality Integrity Availability (CIA) paradigm.

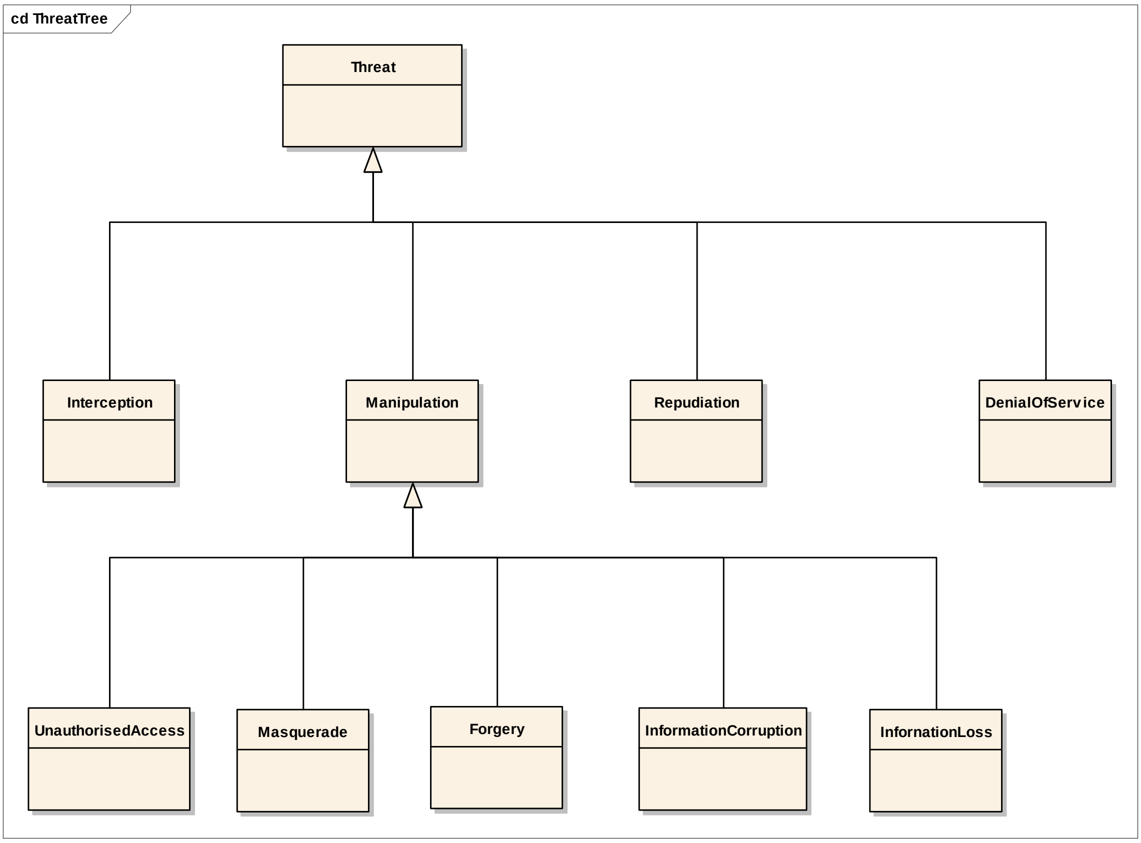

Figure 3: Threat tree

Table 3 shows how the principal CIA security objective classifications are vulnerable to specific types of threat.

Table 3: Threats to security objective types

Threat	Objective type				
	Confidentiality	Integrity	Availability (including sub-classes)		
			Availability	Authenticity	Accountability
Interception (eavesdropping)	X				
Unauthorized access	X	X		X	X
Masquerade	X	X		X	X
Forgery		X	X	X	X
Loss or corruption of information		X	X		
Repudiation		X		X	X
Denial of service			X		

The consequence of the very technical structure of many cyber-security provisions is that the integrated approach to cyber-resilience of the CRA is not explicit. However, it is also noted that there are many guiding principles adopted in the security and security standards development community that are simplified into at least the principles explained in simple terms below:

- Least privilege:
  - Only those entities with a provable need to do something are allowed to do that thing (task, service, etc.). This addresses all aspects of a system such as invoking an application or service, accessing data, etc.

- Least persistence:
  - Any relationship that is intended to be temporary should be designed in such a way that it does not persist after use. The intent is to minimize any risk from enabling/hijacking a dormant process for malicious purposes. For instance, if a process is required to do something then it should only exist for the time required to do that thing.
- Zero Trust:
  - What this means in non-technical terms is do not exchange data or invoke a service belonging to some other entity before verifying the entity. This means verifying its identity, its capability, and any other relevant attribute. Further, zero-trust requires that any established trust relationship is non-persistent and trust is rebuilt every time hence building back into the least privilege and least persistence objectives above.

In addition security design should ensure that systems and components "fail secure" and also "fail safe". In recognizing that forcing a failure is an attack vector in its own right, systems have to be able to "recover secure" whilst also remaining functional and safe. Such complex attack forms (e.g. force failure in component *x* to open a path to component *y*) should be addressed in the system risk analysis (i.e. side channel analysis is critical to success).

EXAMPLE: Whilst guidance is given to keep a key secret and only accessible by algorithms, it has been shown that analysis of the thermal properties of circuits can identify the memory location of the key and then applying further analytic tools, e.g. side channel power analysis, it can be assessed if the memory is storing a 1 or a 0 and then the key can be recovered. Mitigations to address such attacks are often not standardized but are part of the state of the art of product design and failure to implement such mitigations may leave crypto-keys vulnerable, hence putting the cryptographic functions at risks even when the algorithm follow best practices.

In general, side channel attacks are the most straightforward way to overcome cybersecurity protections and therefore security designers also should look at the likelihood of a side channel attack and build countermeasures for those into the design. The obvious question is if side-channel attacks are adequately covered in guidance and in risk analysis? Protection against side channel attack is an implementation matter not affecting interoperability and requiring specific know-how, and therefore not naturally addressed by standards organizations. This raises an interesting question about the role of SDOs and of standards addressed in more detail in clause 4.2.

6.2 Are standards meant as education material?

Standards generally do not say why something has to be done, rather they simplify the text to a set of strong recommendations (modal verb should) and mandates (modal verb "shall"). The guidance documents from SDOs also are not often tutorial in nature - there is an assumed level of expertise in the subject matter. However one of the concerns raised, and underpinning the CRA [i.1], is the lack of knowledge in the wider community about the application of security techniques (the key assertion of this study is that there is no lack of measures available). This is quite strongly stated in the red box (see figure 1 of the present document) that states "*insufficient understanding among users as regards the cybersecurity of products*" and in the blue boxes "*manufacturers do not provide information on security problems and vulnerabilities*", and "*manufacturers do not provide information on secure use*". The gap between a standard existing and being precise in its application, to the knowledge required to both be aware of it and to use it appears significant (as written in the CRA). This is a knowledge gap that can be usefully closed.

The bulk of standards are developed as the minimum essential set of requirements to achieve the desired interoperability goals, or regulatory goals. The expectation of the implementor having sufficient expertise to implement the standard without introducing new vulnerabilities is unstated. It is therefore clear that the CRA places additional expectations on industry to give assurances in this domain and this will have an impact on the standards prepared by industry. It is also reinforced that the authors of standards are most often direct stakeholders in the technology or service enabled by the standards.

As SDOs are populated by subject matter experts it may be reasonable to ask that the SDOs prepare more fundamental guidance. ETSI has begun to address this already in the Education about Standardization thread: https://www.etsi.org/education.

It is clear that a gap exists in getting the market to use security standards. However it is also clear that many cyber-security education programmes exist in tertiary education and that many large organizations have training and awareness programmes for cyber-security.

RECOMMENDATION#3: The role of standards as part of product and service design should be reinforced but should not detract from the primary role of standards to be concise, accurate and testable.

6.3 Security standards frameworks

It can be argued that security measures are fractal or self-similar in nature - no matter the level of magnification the pattern is the same. The CIA paradigm (Confidentiality Integrity Availability) is one example of this as it applies almost equally at every layer of the OSI model, or to every process of an application's code, or to every interaction between people. The set of common features applies equally to the standards that are developed. The rationale is that by using a very small number of common frameworks and making them applicable across as wide a surface as possible then the number of deviations that can be exploited is minimized. This is wholly consistent with the aim of minimizing the attack surface discussed in clause 4.3.1.

The model of a framework standard taken from ETSI EN 303 645 [i.29] is simplified below. The set of common requirements, tools and methods are often referred to as "horizontal standards" with the specializations for any industry sector often referred to as "vertical standards". The simple rule developed from the experience of ETSI EN 303 645 [i.29] is that the common requirements can be extended in preference to allowing for deviation or extension in any vertical or industrial sector (see figure 4).

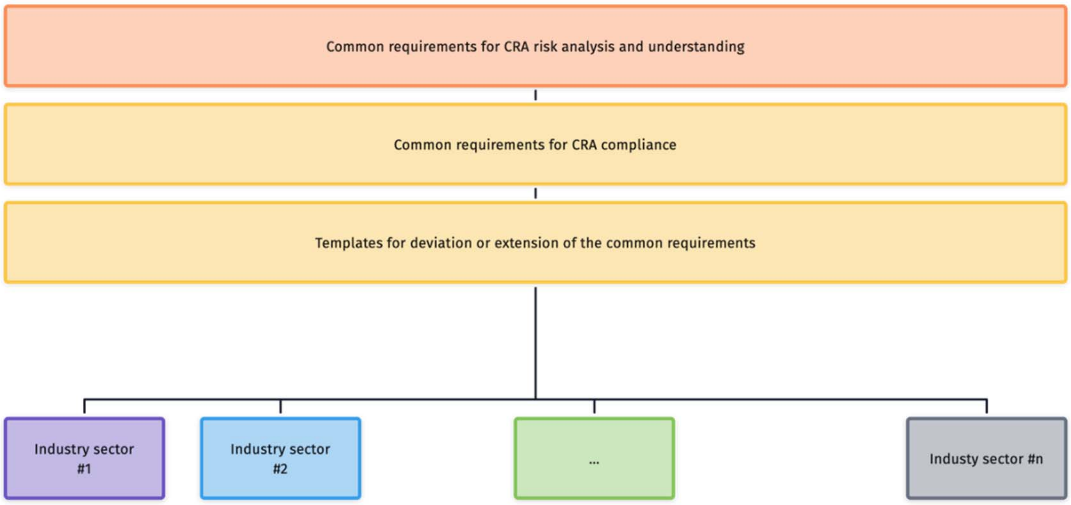
Common requirements for CRA risk analysis and understanding
Common requirements for CRA compliance
Templates for deviation or extension of the common requirements
Industry sector #1
Industry sector #2
...
Industy sector #n

Figure 4: Illustration of ETSI approach for deriving sector specific standards from a common framework

By maximizing the applicability of standards representing the common elements, and by making the template or requirements for when a deviation is allowed, the level of sectorial deviation from the common base is minimized. This then ensures the maximum coverage of security standards from the minimum set of them. Thus the overall available attack surface is minimized consistently across the maximum range of products and services.

There is an additional role for key management frameworks in actually placing products and services on the market. There are a number of ways of distributing cryptographic key material to end users, including the SIM card of mobile phones (and generally the smart-card used in banking), and public key infrastructures. More consideration of the role of ETSI (in particular TC ESI) in such domains is addressed in clause 8.

6.4 Confidentiality protection

Protecting the confidentiality of data is a key problem that has been addressed in the security domain for many centuries. Mechanisms to provide confidentiality of data at rest and in transit are universally available. Furthermore, means to protect data in pre-defined (usually using shared, symmetric, credentials) and in open relationships (usually using asymmetric credential sets) are well specified. Many of these capabilities are further supported by specialized hardware.

EXAMPLE: There are lots of protocols and algorithms to provide confidentiality protection (e.g. the AES algorithm, HTTP/S protocols).

A problem in using such protection is that there is a degree of difficulty in ensuring that the key is protected from exploit. Whilst there is a lot of guidance on not using weak passwords, not using default passwords, and so forth, it is often difficult to verify. So, whilst it is possible to state that standards exist to assure that protected data is always confidential and accessible only to the key holder, it is not always possible to guarantee that the key user is the legitimate key holder.

ASSERTION: Mechanisms exist, documented in standards, that allow for prevention of attacks on data confidentiality, that when implemented support the CRA requirement to "*protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state-of-the-art mechanisms*".

NOTE: If data is encrypted the encryption prevents the attacker getting access to the information content of the data.

6.5 Protection against manipulation attacks

As suggested in the threat tree above there are many forms of manipulation attack and, again, there are many standards that are widely available that can counter such attacks.

EXAMPLE: The hash algorithms such as SHA, when properly used, can be used to detect if an attacker has manipulated data.

The key phrase here is "properly used" as it is easy to apply a hash algorithm but offer no security.

ASSERTION: Mechanisms exist, documented in standards, that allow for prevention of manipulation attacks. Such mechanisms when implemented support the CRA requirement to "*protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, as well as report on corruptions*".

In some use cases, such as in supply chain management, or ledger management, there is extensive work being developed on SBOMs (e.g. in ETSI CYBER) and on Permissioned Ledgers (e.g. in ETSI ISG PDL).

6.6 Identity protection

Identity is a complex construct and in technical standardization is often reduced to the protection of identifiers. Ongoing work in ETSI in ETSI TS 103 486 [i.31], in SmartM2M for SAREF and similar, allow for management of identity and associated identifiers, including the relationships between identifiers. In particular, the nature of identity where context and semantics play a role is key and may lead to a complex mitigation. Identification of natural and legal persons, supporting legal accountability for their actions, is addressed in the eIDAS regulation (Regulation EU 910/2014 [i.13] on electronic identification, authentication and signatures) including a recent amendment establishing a framework for a European Digital Identity.

NOTE 1: The role of identity is complex and in general technical standards do not define identity per se, but give assurance that the proffered identifier can be contextually trusted to be valid.

NOTE 2: Significant work has been carried out in ETSI and CEN on the current eIDAS regulation, with further work being carried out in support of the revised regulation on EU Digital Identity Framework, covering identity in Digital Signatures and use of EU Digital Wallet for the identification of natural and legal person (see clause 8 for an overview of existing work). At the time of preparing the present document the amendment to eIDAS establishing a framework for a European Digital Identity is undergoing final approval in parliament.

ASSERTION: Mechanisms exist, documented in standards, that allow for mitigation of identity attacks. Such mechanisms when implemented support the CRA requirement to "*ensure protection from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems*".

6.7 Denial of service mitigations

In ETSI TS 102 165-2 [i.30] (and earlier editions of ETSI TS 102 165-1 [i.9]) there is extensive text on denial of service attacks and mitigations. In the slightly wider interpretation of denial of service at the content level by misdirection, or evasion in AI systems, work is being developed in ETSI's TC SAI (note that in December 2023 TC SAI inherited the workplan of ETSI ISG SAI) that will provide wider mitigations of network layer DoS. This will address DoS by attacks that achieve their goals in slightly different modes to those at the communications layers.

In addition, for most radio-based systems developed in ETSI (or as part of a partnership project such as 3GPP) systems to mitigate denial of access are built into the frequency (for FDMA systems), code (for CDMA) or timing (for TDMA), or any combination thereof, to mitigate DoS attacks. In router based telecommunications systems (e.g. Internet Protocol) some native ability is engineered into the system that allows for some form of DoS mitigation (e.g. by message filtering).

ASSERTION: Mechanisms exist, documented in standards, that allow for identification and mitigation of denial of service attacks. Such mechanisms when implemented support the CRA requirement "*protect the availability of essential functions, including the resilience against and mitigation of denial of service attacks*".

7 Proof and validation of security standards

The convention in standards is that if a technical specification contains a requirement it has to be testable. However, whilst testing of a protocol or physical properties is relatively straightforward as the environment is immutable and the test can be repeatable, this does not necessarily apply to a claim of "it is secure". In the long list of standards gathered by ENISA/JRC and analysed in the development of Annex A of the present document only a handful of instances of the word test appear out of the 190 or so standards listed. Only 1 Protection Profile is listed. No listings exist for test suite purposes or test cases. In addition, as noted in clause 4.5, the role of conformance and of standards often cites test standards as opposed to baseline standards (e.g. most HSs cited in the EU Official Journal are test standards).

There is therefore a gap between the normal expectation of test suites and test cases as used in many harmonised standards against which a claim of regulatory conformance can be made and what is available for security. There is similarly no guidance in the form of protection profiles for the majority of the base standards to guide an evaluator.

This has been addressed in recent months in ETSI TC CYBER with the adoption of new work items for development of PPs for specific classes of equipment and extension of the guidance for development of analysis against the risk and vulnerability assessments expected for the CSA.

It is also noted that ETSI has developed a number of formal and semi-formal languages for use in the definition of tests. These include TPLan (ETSI ES 202 553 [i.32]), used in the development of test purposes for both conformance and interoperability testing, the Test Description Language (TDL) used for describing test cases, and TTCN used for the detailed definition of executable test cases. Wider adoption of these tools will improve the testing coverage of the security provisions in standards.

What this means with respect to the CRA is that whilst clause 6 asserts that mechanisms exist that are documented in standards to mitigate threats across the CIA paradigm there is very little formal validation of these in any specific application (in part as the context of an implementation has a direct impact on the efficacy of measures). There is increasing attention being paid across ETSI to the development of protection profiles (PPs), both as straightforward technical documents, but also to have the PP validated. This is being addressed in TC CYBER and in TC ESI and recognized as essential in domains including ITS where ETSI standards form the technical basis of some PPs that have been prepared by external but cooperating organizations.

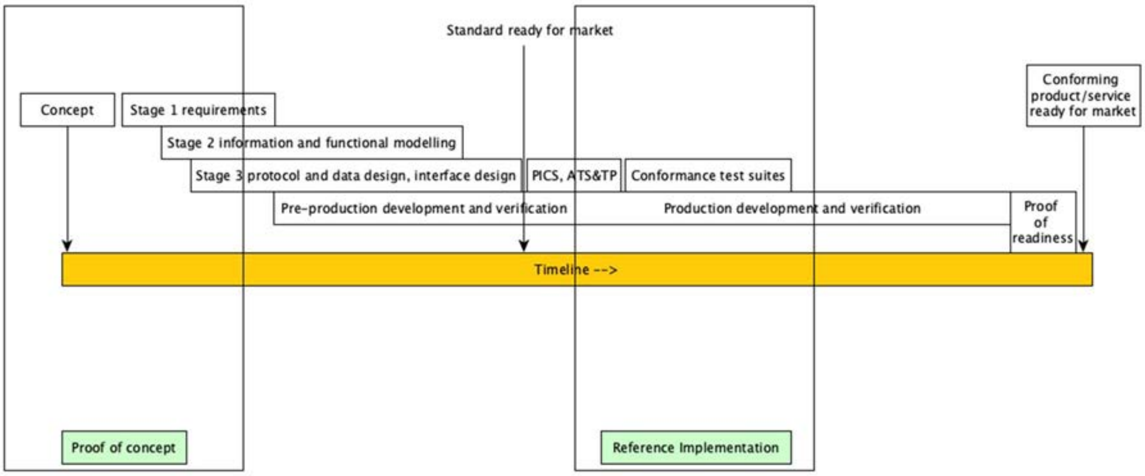
Standard ready for market
Concept
Stage 1 requirements
Stage 2 information and functional modelling
Stage 3 protocol and data design, interface design
PICS, ATS&TP
Conformance test suites
Pre-production development and verification
Production development and verification
Proof of readiness
Conforming product/service ready for market
Timeline -->
Proof of concept
Reference Implementation

Figure 5: Staged process of standards development (historic)

The standards development cycle has evolved over the years but can be approximated by the timeline shown above (see figure 5). The stage 3 elements shown above for the test and verification can also be developed in an ISO/IEC 15408 [i.45] conformant style as a Protection Profile (PP) that expand the base requirements into phrasing as Common Criteria specific Security Functional Requirements, in addition the structure of test purposes and test cases in the CC/PP environment are slightly different from those historically used in ETSI standards.

The impact of the CSA and the role of such market access controls as the EUCC (the cybersecurity certification scheme for Europe based on Common Criteria) suggests that increasing attention should be paid to the role of evaluation and certification. This is being addressed across ETSI and its partners (e.g. in CYBER, in ESI and in ITS).

ETSI has acquired experience in standardizing Common Criteria Protection Profiles, as attested by the ETSI TS 103 732-1 [i.33] Consumer Mobile Device PP developed by ETSI TC CYBER further complemented by optional modules e.g. ETSI TS 103 732-2 [i.47] for Biometry. It is however noted that PPs are essentially statements of requirements and have broad similarities to the conventional standards prepared by ETSI as ESs, TS, and ENs. This has been stated in ETSI EG 203 367 [i.48]. For placement on the market, it may be necessary to have legal certainty regarding conformance to some standard. For domains such as cybersecurity where there are no strict physical constraints on the ability of a system to be attacked, a claim of being secure cannot be maintained over time. The role of testing, and of measurement, is critical in any engineering process. For security, as the underlying attack surface changes over time, any test that assumes a static condition will give an unsafe verdict (i.e. the verdict cannot be relied on over time). As cybersecurity (or more precisely the act of ensuring something is free from cyberattack) is a process, then there are aspects of continuous measurement that apply as opposed to a static test. For assurance that a system offers reasonable security, the processes also should be assessed. Thus, for security, there has to be a balance between what can be tested independently of the environment, e.g. algorithms and protocols, and those which can only be tested within a specific environmental context. It has been suggested that testing and evaluation are approaches to giving a verdict that an implementation conforms to a set of requirements. In the PP domain the evaluator reaches the verdict, whereas in the world of testing against physical criteria, automated testing often suffices. For cybersecurity, both approaches should be taken in combination. Thus, both formal test suites (e.g. as used in the ITS domain and found in ETSI TS 103 096 [i.49]) and Protection Profiles (e.g. as found in CYBER TS 103 732 parts 1 [i.33], 2 [i.47] and 3 [i.50] or in QKD in ETSI GS QKD 016 [i.51]). (See also figure 6).

EXAMPLE: Measures for safety are often based on directly measurable phenomena such as the level of a contaminant in drinking water (parts per million say), or the deflection of a metal rod of known dimensions under load. If the level of contamination in water is below the prescribed limit the verdict is pass (i.e. safe to drink), or if the deflection of the metal rod is below the limit the verdict is pass (i.e. the rod is rated suitable for particular applications).

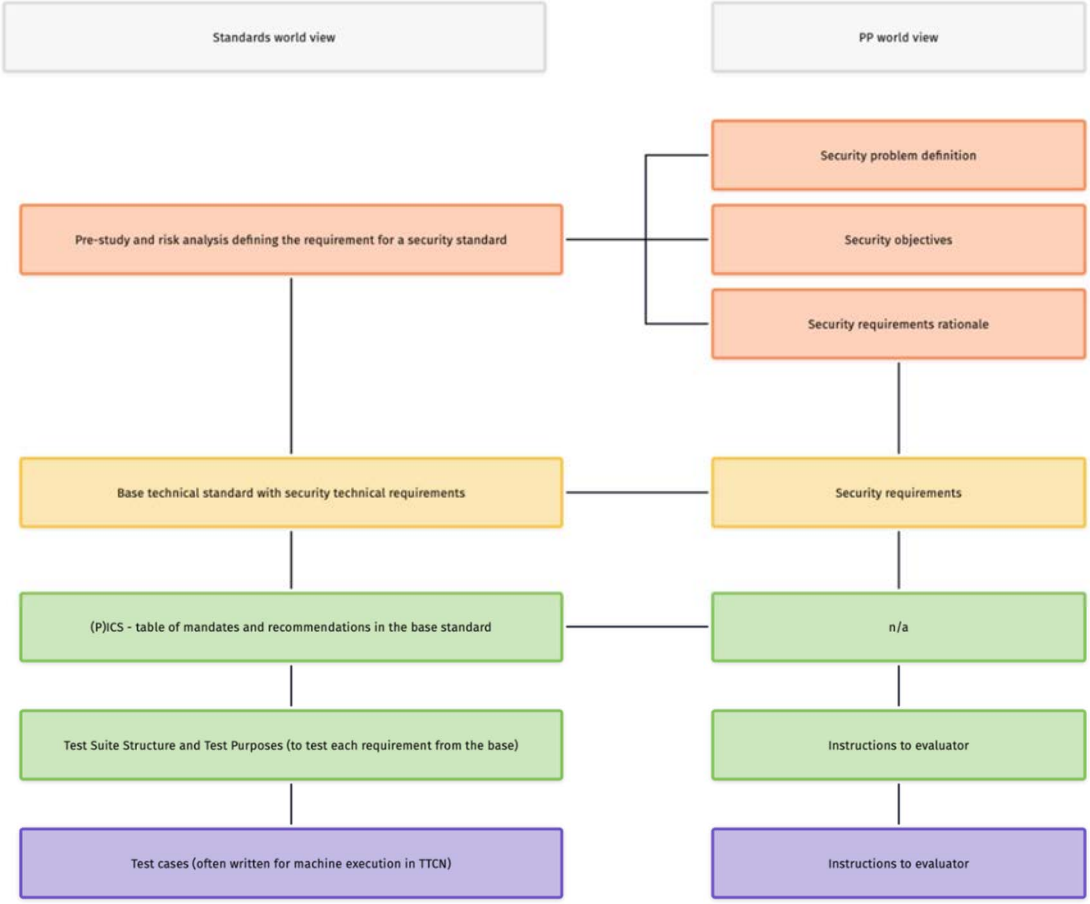
Standards world view
PP world view
Security problem definition
Pre-study and risk analysis defining the requirement for a security standard
Security objectives
Security requirements rationale
Base technical standard with security technical requirements
Security requirements
(P)ICS - table of mandates and recommendations in the base standard
n/a
Test Suite Structure and Test Purposes (to test each requirement from the base)
Instructions to evaluator
Test cases (often written for machine execution in TTCN)
Instructions to evaluator

Figure 6: Indicative comparison of document content in ETSI and PP approaches

8 Trust and digital signature frameworks

Whilst the CRA does not call out any capabilities specific to digital signature, nor does it explicitly cite any interaction with the eIDAS frameworks, the present document makes assertions with regards to the role of Electronic Signatures and Seals in the support of the protection of digital elements. In addition the present document recognizes that in order to provision any form of asymmetric cryptography, as used in many security services, there is a requirement to provide a supporting infrastructure and policy framework (see also figure 7).

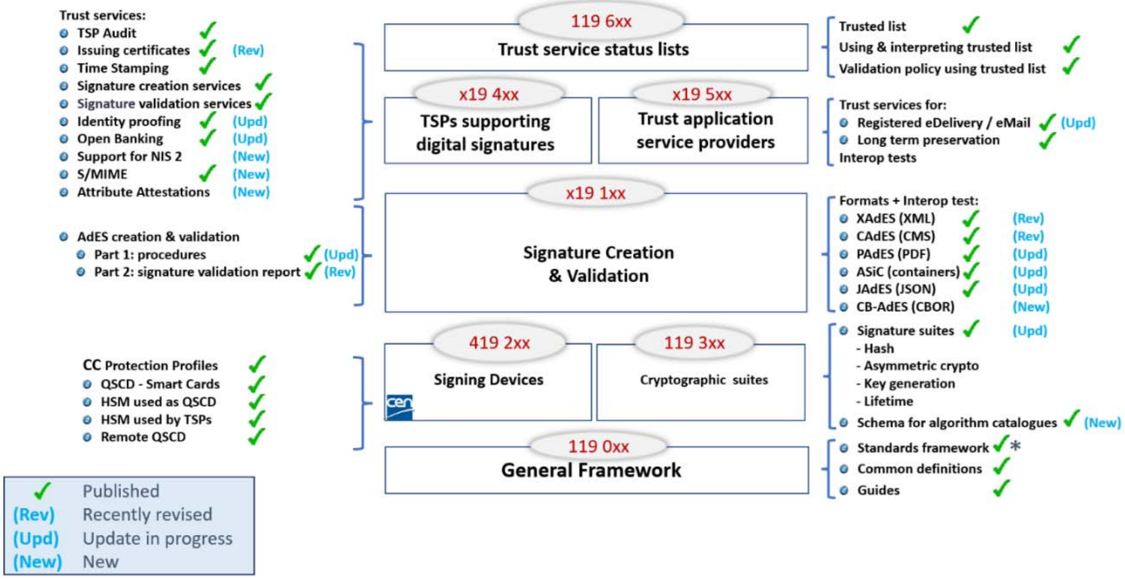

Figure 7: Standards map for trust and signature services

In addressing the standardization request that accompanies the CRA the following observations are made with respect to work of ETSI's TC ESI against items 3, 5, 14 and 15 of SR and summarized below.

Table 4: Mapping of ESI work items against specific items of the initial draft CRA Standardization Request

Reference information from CRA SR		Areas that TC ESI may contribute
Product-agnostic standards for security requirements relating to the properties of products with digital elements		
3.	European standard(s) and/or European standardization deliverable(s) on ensuring protection of products with digital elements from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems	**Horizontal** Direct relevance to: • **EU Digital Identity Wallets** with **electronic attribute attestations** for controlling access to remote services. • Techniques for **identity proofing** for registration of identities.
5.	European standard(s) and/or European standardization deliverable(s) on protecting the integrity of personal or other data, commands, programs by a product with digital elements, and its configuration against any manipulation or modification not authorized by the user, as well as reporting on corruptions	**Horizontal** Direct relevance to: • Any standard that defines and / or uses digital signature. • Digital signatures used to assure data integrity. • Working with ISG PDL on use of distributed ledgers to ensure integrity of data. • Application of IAM to access control e.g. on **e-Delivery** and on **remote signing** trusted services.
14.	European standard(s) and/or European standardization deliverable(s) on essential cybersecurity requirements for identity management systems software and privileged access management software	**Horizontal** Direct relevance to: • **EU Digital Identity Wallets** with **electronic attribute attestations** for controlling access to remote services. • Techniques for **identity proofing** for registration of identities.
15.	European standard(s) and/or European standardization deliverable(s) on essential cybersecurity requirements for standalone and embedded browsers	**Horizontal** Direct relevance to: • Website authentication techniques to be supported by web browsers. In particular, **authentication of person/organization behind website**.

It is strongly asserted that many of ETSI ESI's standards can also contribute from a horizontal view to a vertical view on the assertion that cybersecurity is an essential element of all ETSI standards for trust services, in particular noting that Qualified Trust Services are considered as critical including for compliance with NIS2 regulation.

- ETSI EN 319 401 [i.34]:
  - This standard can be used as base requirements for Cyber Security for all trust services (qualified and non-qualified), and at the time of preparation of the present document is being updated to fully comply with NIS2 [i.2].
- ETSI EN 319 403-1 [i.52]:
  - This Standard for conformity assessment of trust services is applicable to all recognized best practice (defined as policy and security requirements).

It is further recognized that ETSI EN 319 401 [i.34] and ETSI EN 319 403-1 [i.52] can be applied to other critical infrastructure services subject to appropriate review.

Annex A:
Indicative mapping of ETSI standards to CRA

A.1 Overview

As indicated in the main body of the present document there are a number of themes running through the CRA that are re-summarized here with an indicative listing of the current ETSI documents or open work items that apply.

NOTE: The listings of specific standards are only indicative to show that there is relevant ETSI activity that can be further developed, other standards from ETSI's catalogue may also apply to each theme.

Table A.1: Mapping of ETSI publications and activity to CRA themes

Theme	**ETSI documents**	
	Base standard	**Test/verification standard**
Risk analysis	Risk assessment methodology: ETSI TS 102 165-1 [i.9] (TVRA method), and ETSI TR 103 935 [i.12] (Assessment of cyber risk based on products' properties to support market placement).	
Generic security	Generic (horizontal) requirements in ETSI EN 303 645 [i.29]. Frameworks for mitigation measures in ETSI TS 102 165-2 [i.30].	Base standard verification in ETSI TS 103 701 [i.35]
Maintaining security (including vulnerability reporting)	Security updates: TC RRS work on Software Reconfiguration and software update solution available as a baseline. On top, the definition of a Radio Application Package as specified in ETSI TS 103 850 [i.36], specifies a container to deliver software code including security requirements, etc. For vulnerability reporting the content of ETSI TR 103 838 [i.23] applies.	
Product specific	ETSI EN 303 645 [i.29] specialization templates Smart Door lock Voice-controlled devices and functions, ETSI TS 103 848 [i.53] Home Gateways Security Requirements ETSI TS 103 931 [i.54] Network Routers security requirements.	Consumer mobile device ETSI TS 103 732 parts 1 [i.33], 2 [i.47] and 3 [i.50] (Protection Profiles)
Network and device management	3GPP SA3 (mobile network security and privacy) and SA5 (mobile networks Management, Orchestration & Charging) work ETSI Zero Touch Network and Service Management (ZSM): Group Report ETSI GR ZSM 010 [i.37] (published July 2021) identifies potential security threats related to the ZSM framework and solutions and proposes mitigation options that should be considered by the ZSM specifications to ensure that the automated processes are secured and deliver the intended business outcomes. The report introduces countermeasures and potential requirements to address the threats and risks. Building on work in ETSI GR ZSM 010 [i.37], the new draft on security aspects (ETSI GS ZSM 014 [i.38]) specifies security capabilities for the ZSM framework architecture	

In conclusion, all core themes of the CRA can be mapped to some form of ETSI standard.

A.2 ETSI standards and activity mapping to CRA Standardization Request

The content of the CRA standardization request in table A.2 is subject to change. The understanding captured in the present document is that standardization deliverables need to have, probably in their scope statement, a clear link to the statement in the standardization request. This may mean that many standards meet the intent of the standardization request (or alternatively there does not need to be one standard per entry in the table).

EXAMPLE: "*delivering products with digital elements without any known exploitable vulnerabilities*" means that the scope of the deliverable makes clear that the deliverable will allow a conformant implementation to claim to have no known vulnerabilities.

Table A.2: Consideration of ETSI standards mapping to CRA Standardization Request

Product-agnostic standards for security requirements relating to the properties of products with digital elements			
Item	**European standard(s) and/or European standardization deliverable(s) on…**	**Due date**	**ETSI standards that may apply and lead ETSI TB**
1	delivering products with digital elements without any known exploitable vulnerabilities	31/05/2025	ETSI has followed a general principle that standards are developed against an understanding of the risk (using the TVRA approach or an equivalent). Any implementation that conforms to an ETSI security standard therefore by default inherits the risk analysis performed in informing the development of the standard. As an SDO there is no direct control on the implementation of the standard where additional vulnerabilities may be introduced.
2	delivering products with digital elements with a secure by default configuration, including the possibility to reset the product to its original state	31/05/2025	… CYBER
3	ensuring protection of products with digital elements from unauthorized access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems	31/05/2025	Many ETSI standards provide mechanisms to provide authentication and access control. As noted in item 1 above the provision of such mechanisms is guided by an understanding of the risk. A general framework for prevention of unauthorized access is addressed in ETSI TS 102 165-2 [i.30] and more detailed mechanisms are addressed across ETSI's output for specific domains. Many of the mechanisms for trust frameworks addressed in ESI standards (as outlined in table 4 of clause 8) also apply.
4	protecting the confidentiality of data, personal or other, stored, transmitted or otherwise processed by a product with digital elements, such as by encrypting relevant data at rest or in transit by state of the art mechanisms	31/05/2025	Many ETSI standards provide mechanisms to provide confidentiality. As noted in item 1 above the provision of such mechanisms is guided by an understanding of the risk. A general framework for confidentiality protection mechanisms is addressed in ETSI TS 102 165-2 [i.30] and more detailed mechanisms are addressed across ETSI's output for specific domains.
5	protecting the integrity of personal or other data, commands, programs by a product with digital elements, and its configuration against any manipulation or modification not authorized by the user, as well as reporting on corruptions	31/05/2025	Many ETSI standards provide mechanisms to provide protection of the integrity of data in any format. As noted in item 1 above the provision of such mechanisms is guided by an understanding of the risk. A general framework for provision of integrity check measures and their verification is addressed in ETSI TS 102 165-2 [i.30] and more detailed mechanisms are addressed across ETSI's output for specific domains. Many of the mechanisms for trust frameworks addressed in ESI standards (as outlined in clause 8) also apply
6	processing only personal or other data that are adequate, relevant and limited to what is necessary in relation to the intended use of the product with digital elements ('minimization of data')	31/05/2025	As noted in item 1 above the provision of standards in ETSI is determined by a risk analysis activity (e.g. the TVRA). ETSI standards have consistently only defined the minimum set of data to achieve operation. If an implementation chooses to expose additional data that would not be known to ETSI.

7	protecting the availability of essential functions of the product with digital elements, including resilience against and mitigation of denial of service attacks	31/05/2025	As noted in item 1 where ETSI develops standards for security against a risk analysis, and where it is identified that availability protections are required then relevant standards will be developed. In this regard the frameworks in, for example, ETSI TS 102 165-2 [i.30], and many of the link monitoring capabilities offered in radio (for example), are designed to directly mitigate such concerns.
8	minimizing the negative impact of a product with digital [sic] elements on the availability of services provided by other devices or networks	31/05/2025	As also noted in item 1, when risk analysis is undertaken, the environment in which a digital element is deployed is expected to be in scope of the analysis and thus any impact of that environment is considered on the specification of any mitigating functions in standards.
9	designing, developing and producing products with digital elements with limited [sic] attack surfaces, including external interfaces	31/05/2025	As noted in item 1 and in item 6, and discussed in some detail in clause 4.3.1 of the present document, the goal is to minimize the attack surface.
10	designing, developing and producing products with digital elements that reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques	31/05/2025	As noted in item 1, item 6 and item 9 the goal of standardization of mitigation is to reduce the impact as far as is possible of any attack.
11	providing security related information by recording and/or monitoring relevant internal activity of products with digital elements, including the access to or modification of data, services or functions	31/05/2025	A consequence of the good practice identified by each of items 1, 6 and 9, and the practical measures introduced in items 3, 4, 5, 7 and others is that the efficacy of functions is monitored. Such practice is routinely standardized.
12	ensuring that vulnerabilities in products with digital elements can be addressed through security updates, including, where applicable, through automatic updates and the notification of available updates to users.	31/05/2025	In undertaking risk based assessments for the purpose of standards, and in accepting that the exposed risk changes over time (by changes in the likelihood of attack), then it is also accepted that mitigations will need to be updated over time. In this regard there exist standards for distribution and update of digital elements across the ETSI portfolio.
Standards for vulnerability-handling requirements			
13	Vulnerability handling for products with digital elements	31/05/2025	A number of standards exist and are being expanded to ensure that stakeholders across the product lifecycle are able to report, handle and exchange information about vulnerabilities. The primary document that applies is ETSI TR 103 838 [i.23] and the functionality is also mandated in the ETSI EN 303 645 [i.29] family of standards. It is noted that ETSI TR 103 838 [i.23] refers to ISO/IEC 29147 [i.39] which, from a vendor perspective, can be complemented with ISO/IEC 30111 [i.40] and ISO/IEC TR 5895:2022 [i.55] to provide an overall view on vulnerability handling.
Product-specific standards for security requirements relating to the properties of products with digital elements			
	European standard(s) and/or European standardization deliverable(s) on essential cybersecurity requirements for…		
	The set of product specific standards listed below are expected to build on common building blocks. For example securing web-browsers will use many of the technologies standardized in ETSI ESI and which are coordinated with the major web-browser developers. In like manner things such as password managers will inherit standards developed for key generation, random number generation, secure storage and so forth. Where no specific entry is given in the 4th column this text applies.		

14	Identity management systems software and privileged access management software	31/05/2026	Many of the mechanisms for trust frameworks addressed in ESI standards (as outlined in table 4 of clause 8) apply.
15	Standalone and embedded browsers	31/05/2026	Many of the mechanisms for trust frameworks addressed in ESI standards (as outlined in table 4 of clause 8) apply.
16	Password managers	31/05/2026	
17	Software that searches for, removes, or quarantines malicious software	31/05/2026	
18	Products with digital elements with the function of virtual private network (VPN)	31/05/2026	
19	Network management systems	31/05/2026	
20	Network configuration management tools	31/05/2026	
21	Network traffic monitoring systems	31/05/2026	
22	Management of network resources	31/05/2026	
23	Security Information and Event Management (SIEM) systems	31/05/2026	
24	Updating and patch management, including boot managers	31/05/2026	
25	Application configuration management systems	31/05/2026	
26	Remote access/sharing software	31/05/2026	
27	Mobile device management software	31/05/2026	
28	Physical network interfaces	31/05/2026	
29	Operating systems, including specifically operating systems for servers, desktops, and mobile devices	31/05/2026	
30	Firewalls, intrusion detection and/or prevention systems, including specifically those intended for industrial use	31/05/2026	
31	Routers, modems intended for the connection to the internet, and switches, including specifically those intended for industrial use	31/05/2026	
32	Microprocessors, including specifically general-purpose microprocessors and microprocessors intended for integration in programmable logic controllers and secure elements	31/05/2026	
33	Microcontrollers	31/05/2026	
34	Application Specific Integrated Circuits (ASIC) and Field-Programmable Gate Arrays (FPGA) intended for the use by essential entities of the type referred to in [Annex I to the Directive XXX/XXXX (NIS2)]	31/05/2026	
35	Industrial Automation & Control Systems (IACS), such as Programmable Logic Controllers (PLC), Distributed Control Systems (DCS), Computerized Numeric Controllers for machine tools (CNC) and Supervisory Control And Data Acquisition systems (SCADA), including specifically those intended for the use by essential entities of the type referred to in Annex I to the Directive (EU) 2022/2555 [i.2])	31/05/2026	
36	Industrial Internet of Things devices, including specifically those intended for use by essential entities of the type referred to in Annex I to Directive (EU) 2022/2555 [i.2])	31/05/2026	ETSI's activity on Consumer IoT has been aligned with activity in IEC relating to IIoT.
37	Hypervisors and container runtime systems that support virtualized execution of operating systems and similar environments	31/05/2026	
38	Public key infrastructure and digital certificate issuers	31/05/2026	This domain is already well managed in ETSI's ESI group. In addition the policy elements of PKIs are often coordinated between ETSI and external partners (e.g. ETSI TC ITS and the EU ITS Policy team).

39	Secure elements	31/05/2026	ETSI's Secure Element Technologies is the natural home of this activity and has a significant work programme already. https://portal.etsi.org/TB-SiteMap/scp/scp-tor
40	Hardware Security Modules (HSMs)	31/05/2026	As above with respect to ETSI SET and with the collaboration between ETSI and industry bodies (e.g. Global Platform).
41	Secure cryptoprocessors	31/05/2026	
42	Smartcards, smartcard readers and tokens	31/05/2026	See line 38.
43	Robot sensing and actuator components and robot controllers	31/05/2026	
44	Essential cybersecurity requirements for smart meters	31/05/2026	

Annex B:
International standards from ITU

Notwithstanding that the primary purpose of the present document is to consider the output of ETSI and the work programme of ETSI in support of the CRA, it is recognized that ETSI has a relationship with the ITU, primarily with ITU-T and ITU-R (for radio). It is further recognized that there are a very large number of ITU publications and areas of work that also map to the CRA. Therefore, this annex provides a summary of the main areas identified in the CRA where there is an expectation of standardization, and some indicators of work from ITU that may apply.

The format follows that offered in clause A.1 (table A.1) of the present document in identifying themes from the CRA and mapping those themes to work in ITU. As also noted in clause A.1 the mapping is only indicative and many other publications from ITU may be cited against each theme.

Table B.1: Indicative mapping of CRA Themes to ITU activity

Theme	ITU documents or work area
Risk analysis	X.1250 [i.56], Common vulnerabilities and exposures X.1055 [i.57], Risk management and risk profile guide
Generic security	X.1205 [i.58, Overview of cybersecurity]
Maintaining security (including vulnerability reporting)	
Product specific	X.1332 [i.59], Security guidelines for smart metering service in smart grids X.1642 [i.60], Guidelines for the operational security of cloud computing
Network and device management	

History

Document history		
V1.1.1	March 2024	Publication