The relationship between the CSA certification framework and cybersecurity requirements in the current EU regulatory landscape

A CORAL project deliverable

Co-financed by the Connecting Europe Facility of the European Union

Document working group

Name	Affiliation	Role
Dr. Shyam Wagle	ANEC GIE	Contributor
Mrs. Natalia Cassagnes	ANEC GIE	Contributor
Dr. Jean Lancrenon	ILNAS	Contributor
Dr. Gabriela Gheorghe	LHC	Reviewer

Document history

Version	Date	Changes from previous
0.1	21/08/2023	Creation of document.
0.10	30/10/2023	Near-finalization of draft.

European Union funding

The CORAL project - of which this deliverable is a part - is Action no. 2020-LU-IA-0209, benefitting from European Union funding under the 2020 CEF Telecom Call[1].

The contents of this publication are the sole responsibility of the ANEC GIE and do not necessarily reflect the opinion of the European Union.

Acronyms

Acronym	Full meaning
AI	Artificial Intelligence
AIA	Artificial Intelligence Act
ANEC GIE	*Groupement d'Intérêt Economique Agence pour la Normalisation et l'Economie de la Connaissance*
CORAL	cybersecurity Certification based On Risk evALuation and treatment
CRA	Cyber Resilience Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
DORA	Digital Operational Resilience Act
EHDS	Proposal for a Regulation on the European Health Data Space
eIDAS	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
eIDAS2	Proposal for a Regulation amending eIDAS as regards establishing a framework for a European Digital Identity
ENISA	European Union Agency for Cybersecurity
ICT	Information and Communication Technology
NIS2	Directive for a High Level of Cybersecurity across the Union

[1] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity

Contents

1. Introduction

The CORAL project

The *cybersecurity Certification based On Risk evALuation and treatment* (CORAL) project (Action no. 2020-LU-IA-0209, benefitting from EU funding under the 2020 CEF Telecom Call[2]) aims to elaborate a toolkit and methodology to support the certification process in line with the Regulation (EU) 2019/881 (Cybersecurity Act - CSA)[3] in what concerns the self-certification and the basic level of assurance, as well as to enhance the exchange of good practices, collaboration and information sharing related to performing evaluations in line with this act. In particular, this project develops a light, efficient and straightforward evaluation method in line with the technical objectives of Article 51 of the CSA and based on risk assessments, to help SMEs achieve a 'basic' assurance level in the cybersecurity of their ICT product, process or service. This method can also be used for conformity self-assessments, also possible with the entry into force of the CSA.

The project partners are:

- The Luxembourg House of Cybersecurity[4] (LHC);
- The *Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services* (ILNAS)[5] ; and
- The *Agence pour la normalisation et l'économie de la connaissance* (ANEC GIE)[6].

More information on the CORAL project and its partners can be found on the project website: https://coral-project.org/

Purpose and scope of this CORAL deliverable

Objective

This deliverable surveys certain existing or upcoming European Union legislative acts that may benefit from CSA certification, and places these in a single resource. The acts – or draft acts available at the time of writing – are first summarized; afterwards, key parts of the acts wherein CSA certification or conformity self-assessment may be of use are pointed to. Finally, we also indicate in which acts CORAL may be useful, taking into account the fact that CORAL's tools and methodology are built for the 'basic' level of assurance.

[2] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom/apply-funding/2020-cybersecurity
[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) https://eur-lex.europa.eu/eli/reg/2019/881/oj
[4] https://lhc.lu/
[5] https://portail-qualite.public.lu/fr/acteurs/ilnas.html
[6] https://portail-qualite.public.lu/fr/acteurs/gie-anec.html

Scope

The legislative texts considered below were selected as follows. A search was performed on the EUR-Lex website[7] using the keywords "certification" and "cybersecurity", and by explicitly seeking Regulations, Directives, proposals for a Regulation, and proposals for a Directive. Afterwards, manual inspection of the search results allowed eliminating texts that did not appear so relevant (for instance, texts that frame EU funding programs). The texts ultimately considered are:

- The Directive for a High Level of Cybersecurity across the Union (NIS2)[8];
- The proposal for a Regulation amending eIDAS as regards establishing a framework for a European Digital Identity (eIDAS2)[9];
- The proposed Cyber Resilience Act (CRA)[10];
- The proposed Artificial Intelligence Act (AIA)[11];
- The proposed Cyber Solidarity Act[12];
- The Machinery Regulation[13];
- The Digital Operational Resilience Act (DORA)[14]; and
- The proposal for a Regulation on the European Health Data Space (EHDS)[15].

The first four are indicated by the ENISA certification mini-site[16] to bring trust to the market of ICT products, services, and processes across the European Union. It is also important to indicate the proposed targeted amendment to the CSA[17] that essentially adds 'managed security services' as an additional category to the list "'ICT products', 'ICT services', and 'ICT processes'" covered in the existing CSA. Indeed, this amendment can have, for some of the considered texts, some non-trivial impact.

Important disclaimers

The authors stress that in no way does this deliverable affirm that the CSA will for certain apply to a given legislative context. The objective is simply to show examples of where this would make sense. How EU regulatory framework evolves, and how draft legal texts are altered before their adoption, are out of the CORAL project's control.

[7] https://eur-lex.europa.eu/homepage.html
[8] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454
[11] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206
[12] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209
[13] https://eur-lex.europa.eu/eli/reg/2023/1230/oj
[14] https://eur-lex.europa.eu/eli/reg/2022/2554/oj
[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197
[16] https://certification.enisa.europa.eu/
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0208

The authors do not claim to be exhaustive. It is possible that the search criteria do not cover all existing or upcoming legal texts that could be affected by the CSA. The selection of search criteria remains subjective in nature.

Project partner ILNAS has - in the Grand Duchy of Luxembourg - several legal missions, in part originating in EU legislation. This deliverable is not to be taken as an indication that ILNAS' legal missions, or any other assignments, will change in one way or another.

2. Existing or upcoming legislative items that may benefit from the CSA

The Directive for a High Level of Cybersecurity across the Union (NIS2)

The NIS2 Directive came into force in January 2023, replacing the NIS Directive (EU 2016/1148)[18]. It sets a more stringent coherent framework for all supervisory and enforcement activities across Member States, overcoming some shortcomings of its predecessor namely in terms of harmonized implementation. It further aims at improving the resilience and incident response capacities of both the public and private sectors and focuses on cybercrime and European and national cybersecurity management.

A summary of NIS2

The NIS2 directive aims at increasing the European Union's cybersecurity resilience by:

- Obliging Member States to put together cybersecurity strategies;
- Obliging Members States to designate national competent authorities or bodies on cybersecurity, in particularly in cybersecurity response, for instance through national Computer Security Incident Response Teams (CSIRTs); and
- Laying out cybersecurity and risk management requirements for certain identified categories of important or critical entities (for instance in the financial sector, energy sector, ICT service management, digital infrastructure, among others).

How NIS2 can be potentially supported by CSA certification

From the NIS2 text itself

Article 24: Use of European cybersecurity certification schemes. Article 21 of NIS2 lays down requirements and measures for cybersecurity risk management in those categories of entities that are listed as essential or important (in Annexes I and II of NIS2). Article 24 stipulates that The Commission may make it mandatory for such entities to use products, services, or processes that are certified under a CSA scheme in particular to support fulfilling Article 21 requirements. The Commission may even ask that a new CSA scheme be drawn up if necessary.

[18] https://eur-lex.europa.eu/eli/dir/2022/2555

The targeted CSA amendment

In April 2023, the Commission announced a proposal for an amendment to the CSA[19] in order to add 'managed security services' alongside 'products', 'services, and 'processes' as a class in its own right that could be the target of a CSA certification[20]. Managed security services include *penetration testing*, *security consultancy*, *security incident management and response*, and *security auditing*. Two major reasons for this proposed change are:

- Managed security service providers are themselves classified under NIS2 as highly critical (see Annex I of NIS2);
- Managed security services are essential in implementing the requirements of Article 21, as they are typically called upon by other entities to assist in cybersecurity matters.

Note that CSIRTs are themselves Managed security service providers. As a result, the CSIRTs put into place by NIS2 may be the targets of CSA certifications or CSA EU declarations of conformity as well in the context of this proposed amendment.

How CORAL might support NIS2

CORAL might be of direct service to NIS2 in its implementation of Article 24 and Article 21 under the condition that the 'basic' level of assurance be sufficient where certification is required or recommended.

The proposal for a Regulation amending eIDAS as regards establishing a framework for a European Digital Identity (eIDAS2)

eIDAS2[21] is a proposed revision of the eIDAS regulation that aims to further enhance the security and reliability of electronic identification and trust services within the EU. The first version came into force in September 2014 to ensure secure and reliable electronic identification and trust services across the EU. It facilitates electronic interactions between businesses, citizens, and public authorities within the EU. Trust services include electronic signatures, electronic seals, time stamps, electronic delivery service, and website authentication. These are essential for the establishment of legal certainty, trust and security in electronic transactions.

A summary of eIDAS2

eIDAS2 is expected to add to eIDAS a framework and rules for the implementation of European Digital Identity Wallets by Member States. These wallets should be usable by citizens and businesses to allow for seamless and secure electronic identification. Major features include:

- The structure of the European digital identity wallet;
- Requirements to the security and privacy of the wallet by design;
- The 'Once only principle', which essentially states that data to public authorities should not have to be provided more than once;

[19] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0208
[20] https://digital-strategy.ec.europa.eu/en/library/proposed-regulation-managed-security-services-amendment
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0281

- The ability for the digital identity to serve as cross-border identification.

How eIDAS2.0 can be potentially supported by CSA certification

Article 6c: Certification of the European Digital Identity Wallets. Digital Identity Wallets are required to be compliant with the security requirements listed in Article 6a. Article 6c states that the CSA certification of the proposed wallet shall provide a presumption of conformity. Thus, it may be the case that a specific CSA certification scheme on (parts of) a digital identity wallet will be drawn up in the future.

Article 12a: Certification of electronic identification schemes. Article 8(2) of eIDAS lays out the assurance level requirements for electronic identification schemes. Article 12a states that the usage of an appropriate CSA certification scheme can be used to demonstrate the achievement of a specific assurance level. Thus, it may be the case that a specific CSA certification scheme on (parts of) an electronic identity scheme will be drawn up in the future.

How CORAL might support eIDAS2.0

CORAL might be of direct service to eIDAS2 during product development, evaluation and certification (for example European Digital Identity Wallet or electronic identification schemes) under the condition that the 'basic' level of assurance be sufficient where certification is required or recommended.

The Cyber Resilience Act (CRA)

The proposal by the European Commission for a regulation on cybersecurity requirements for products with digital elements[22] was submitted in September 2022. Known as the European Cyber Resilience Act (CRA), it aims to strengthen cybersecurity rules to ensure that secure hardware and software products[23] are placed on the European single market.

A summary of the CRA

The following two main objectives are identified in the CRA proposal aiming to ensure the proper functioning of the internal market:

- create conditions for the development of secure products with digital elements by ensuring that hardware and software products are placed on the market with fewer vulnerabilities and ensure that manufacturers take security seriously throughout a product's life cycle; and
- create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

In addition to main two objectives, four other specific objectives are set out in the CRA proposal:

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

[22] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0454

[23] In the CRA, a product also incorporates its remote data processing solutions. These, however may rely on other products that have to be assessed for market placement separately.

- ensure a coherent cybersecurity framework, facilitating compliance for hardware and software producers;
- enhance the transparency of security properties of products with digital elements, and
- enable businesses and consumers to use products with digital elements securely.

The proposed Regulation lists the essential cybersecurity requirements for all products with digital elements in Annex I, and specifies classes of critical products with digital elements in Annex III. It also states those methods by which conformity assessment of products with digital elements is achieved to demonstrate compliance to the Regulation.

Note. There is an existing directive that may cause the entry into force of the CRA to yield a regulatory overlap: the currently in force Radio Equipment Directive's (or RED[24]) activation of the RED's Article 3(3), points (d), (e) and (f)[25]. It is envisaged that this delegated regulation could be repealed if the CRA applies.

How the CRA can be potentially supported by CSA certification

Article 6: Critical products with digital elements. Paragraph 5 specifies that the Commission can adopt delegated acts in accordance with Article 50 in order to specify that certain classes of critical products with digital elements shall require a CSA certification. It is possible thus that such schemes may need to be drawn up to do so, for specific classes of products.

Article 18: Presumption of conformity. Products with digital elements that are already certified in the context of the CSA or have issued a CSA EU declaration of conformity may be presumed conform to the requirements listed in Annex I, provided that these requirements are correctly covered by the scope of the certificate or declaration.

How CORAL might support CRA

CORAL might be of direct service to CRA for the presumption of conformity according to Article 18 under the condition that the essential or the 'basic' level of assurance be sufficient where certification is required or recommended. (It could also be the case for Article 6, but this may be less likely as it is reasonable to expect that critical products with digital elements be required to achieve a CSA assurance level of 'substantial' or 'high'.)

The AI Act (AIA)

Considering the rapid developments in the area of Artificial Intelligence (AI), the European Commission proposed the Artificial Intelligence Act (AIA), the first EU regulatory framework for AI in April 2021, to regulate AI for ensuring better conditions for the development and use of this innovative technology[26]. It establishes obligations for providers and users of AI depending on the level of risk.

[24] https://eur-lex.europa.eu/eli/dir/2014/53/oj
[25] https://eur-lex.europa.eu/eli/reg_del/2022/30/oj
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206

A summary of the AIA

The proposed AIA classifies AI systems by risk and mandates various development and use requirements. In particular, there are the following four levels of risk in AI[27]:

- Unacceptable risk: Unacceptable risk AI systems are all the AI systems that are considered as a clear threat to the safety, livelihoods and rights of people. Such systems are to be prohibited;
- High risk: All the AI systems that negatively affect safety or fundamental rights will be considered as high risk and will be assessed before being placed on the market and also throughout their lifecycle;
- Limited risk: It refers to all AI systems with specific transparency obligations. In such cases, users should be made aware that they are interacting with a machine so they can make their own decision to continue or step back;
- Minimal or no risk: The AIA allows the free use of minimal-risk or no-risk AI systems without conforming to any additional legal obligations. It includes applications like spam filters or video games which are allowed to be used with little requirements other than transparency obligations.

The AIA also has provisions for cybersecurity requirements, in the particular case of high-risk AI systems; these are set out in Article 15.

How the AIA can be potentially supported by CSA certification

Article 42(2): Presumption of conformity with certain requirements. This article states that High-risk AI systems that have been certified or for which a statement of conformity has been issued under a CSA cybersecurity scheme shall be presumed to be in compliance with the cybersecurity requirements set out in Article 15, assuming these are in the scope of the CSA scheme.

How CORAL might support the AIA

CORAL might be of direct service to AIA in its implementation of Articles 15 and 42 for high risks AI systems for the presumption of conformity under the condition that the essential or the 'basic' level of assurance be sufficient where certification or a CSA EU declaration of conformity is required or recommended.

The Cyber Solidarity Act

In order to strengthen solidarity at the EU level to better detect, prepare for and respond to significant or large-scale cybersecurity incidents, in particular through the creation of a European Cybersecurity Shield and a comprehensive Cyber Emergency Mechanism, the European Commission has adopted a proposal for the EU Cyber Solidarity Act[28] in April 2023[29]. The act is expected to support detection and awareness of cybersecurity threats and incidents, boost preparedness of critical entities, as well as reinforce solidarity, concerted crisis management and response capabilities across Member States. It also establishes EU capabilities to make the Union more resilient and reactive to cyber threats, strengthening

[27] Regulatory framework proposal on artificial intelligence | Shaping Europe's digital future (europa.eu)
[28] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209
[29] https://ec.europa.eu/commission/presscorner/detail/en/IP_23_2243

existing mechanisms and contributing to ensuring a safe and secure digital landscape for citizens and businesses.

A summary of the Cyber Solidarity Act

The Cyber Solidarity Act has the following specific objectives:

- to strengthen common EU detection and situational awareness of cyber threats and incidents in order to contribute to European technological sovereignty in the area of cybersecurity;
- to reinforce preparedness of critical entities across the EU and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making incident response support available for third countries.

To achieve these objectives, the following concrete actions have been proposed:

- The establishment of a European Cyber Shield, a pan-European infrastructure of national and cross-border Security Operations Centres (SOCs) across the EU to detect major cyber threats quickly and effectively; and
- The creation of a Cyber Emergency Mechanism to increase preparedness and enhance incident response capabilities in the EU in order to support for:
    - preparedness actions based on common risk scenarios and methodologies, such as testing entities in highly critical sectors for potential vulnerabilities;
    - creating a new EU Cybersecurity Reserve consisting of incident response services from trusted providers in case of a significant cybersecurity incident; and
    - providing financial support for mutual assistance among member states; and
- The establishment of a Cybersecurity Incident Review Mechanism to enhance Union resilience which is intended to review and assess significant cybersecurity incidents after occurrences and issue recommendations to improve cyber posture.

Of particular interest here is the provisioning of the EU Cybersecurity reserve, laid out in Article 12. It is to be composed of what the Regulation calls trusted providers, the requirements of which are detailed in Article 16.

How the Cyber Solidarity Act can be potentially supported by CSA certification

Article 16(2): Trusted providers. Point (j) highlights that once an EU certification scheme for managed security service Regulation (EU) 2019/881 is in place, the provider shall be certified in accordance with that scheme. (This is also mentioned in Recital 35.) Thus, one can expect that a CSA scheme covering one or more types of managed security service providers shall be drawn up in the future, in accordance with the proposed amendment to the CSA[30] (previously mentioned in the Section on the NIS2 Directive).

[30] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0208

How CORAL might support Cyber Solidarity Act

CORAL could be of direct service to Cyber Solidarity Act assuming at some point that a CSA scheme for managed security services incorporating assurance level 'basic' is made available.

The Machinery Regulation

The Machinery Regulation of 2023[31] aims to regulate the placement on the EU's internal market of certain categories of machinery or partly completed machinery[32], in particular to ensure that these products are adequately safe and to remove obstacles to trade in machinery between Member States.

A summary of the Machinery Regulation

These health and safety requirements concern the design and construction of machinery and related products[33]. The text also specifies rules on the free movement of products within the scope. The products mainly concerned include: interchangeable equipment, safety components, and removable mechanical transmission devices, just to name a few. The essential health and safety requirements relating to the design and construction of those products in scope are detailed in Annex III. Of noteworthy significance are those provisions in Annex II paragraphs 1.1.9 and 1.2.1, where the machinery or product in question may have elements of its software attacked or otherwise corrupted, potentially leading to a hazardous operation or configuration.

How the Machinery Regulation can be potentially supported by CSA certification

Article 20: Presumption of conformity of products within the scope of this Regulation. Article 20(9) highlights that machinery and related products that have been CSA certified or for which a CSA EU statement of conformity has been issued shall be presumed to be in conformity with the essential health and safety requirements set out in Annex III, sections 1.1.9 and 1.2.1, as regards protection against corruption and safety and reliability of control systems insofar as those requirements are applicable.

How CORAL might support this regulation

CORAL might be of direct service to this Regulation in its implementation of Article 20(9) for achieving presumption of conformity, provided that the CSA scheme that is applicable to the Machinery Regulation operates at level 'basic'.

The Digital Operational Resilience for the Financial Sector (DORA)

The Digital Operational Resilience for the Financial Sector (DORA)[34] came into force in December 2022 with the objectives of elevating the financial sector's operational resilience as well as further enhancing

[31] https://eur-lex.europa.eu/eli/reg/2023/1230/oj
[32] "Machinery" in this sense essentially means equipement with moving parts that are actionable with non-human or animal effort, e.g. engine-driven equipment.
[33] Per recital 15 of the Regulation: "related products should be understood as comprising interchangeable equipment, safety components, lifting accessories, chains, ropes and webbing, and removable mechanical transmission devices […]."
[34] https://eur-lex.europa.eu/eli/reg/2022/2554/oj

security requirements to reduce threats and risks deriving from the use of ICT and building up operational resilience of the financial sector against ICT related incidents.

A summary of the DORA

DORA creates a cybersecurity ruleset for a large class of financial entities, e.g. credit institutions, payment and e-money institutions as well as other entities of the financial sector, such as management companies, insurance players, etc. (The full list of targets is specified in Article 2.) All entities in scope are required to assess and comply with an extensive series of requirements regarding ICT aspects, articulated around the following five main pillars[35]:

- ICT risk management;
- ICT-related incident management, including payment-related incidents;
- Digital operational resilience testing;
- Management of ICT third-party risks and oversight of critical ICT third-party service providers; and
- Information and intelligence sharing arrangements.

It is important to note that the DORA focuses on financial institutions, which are expected to ensure that they are prepared to identify, monitor, and most importantly protect themselves from a variety of ICT related risks which are significantly more common nowadays.

How DORA can be potentially supported by CSA certification

DORA does not have any specific mention of CSA certification in its text. However, it remains a text heavily focused on the adequate management of cybersecurity risk, and the detection and proper reporting of incidents and threats. One can consult, for instance:

- Article 6 on the establishment and maintenance of a sound, comprehensive and well-documented ICT risk management framework;
- Article 9 on the adequate protection of ICT systems;
- Article 10 and 11 on incident detection and recovery; and
- Article 13 on learning and evolving, in particular on the tracking of vulnerabilities and the enhancing of cybersecurity maturity; or
- Chapter II, entirely devoted to ICT-related incident management, classification and reporting.

The CSA could logically be of use in two broad categories of activity:

- ICT systems, depending on the risk level, can be built on CSA certified products, services or processes, assuming appropriate CSA schemes are in place;
- Personnel, whether internal or external, providing managed security services in order to run the framework could operate in the context of a CSA-certified managed service security provider,

[35] https://www.digital-operational-resilience-act.com/

again assuming an appropriate scheme to do so is in place, namely through the proposed CSA amendment[36].

The proposal for a Regulation on the European Health Data Space (EHDS)[37]

The proposal for a Regulation on the European Health Data Space (EHDS)[38] is a Regulation that establishes a comprehensive framework to create, at the EU level, a common virtual space for an interoperable and cross-border use of health data across the single market. Thus, the Regulation provides rules, requirements on infrastructures, and governance practices to do so, including setting cybersecurity requirements where appropriate.

A Summary of EHDS

The proposed Regulation concretely:

- Increases citizens' rights regarding the access to and usage of their electronic health data;
- Defines rules for placement in the single market of electronic health record systems; and
- Establishes mandatory infrastructure for cross-border usage of electronic health data.

In particular, requirements and obligations are laid out on EHR manufacturers and providers.

How the EHDS can be potentially supported by CSA certification

The EHDS does not specifically mention the CSA in its articles. However, EHR systems remain ICT systems that manage sensitive data. It is mentioned in Recital 27 that general requirements on cybersecurity should be supported by certain mechanisms, in particular the CSA certification of underlying components or other systems. This would be in addition to other requirements specific to the case of EHR.

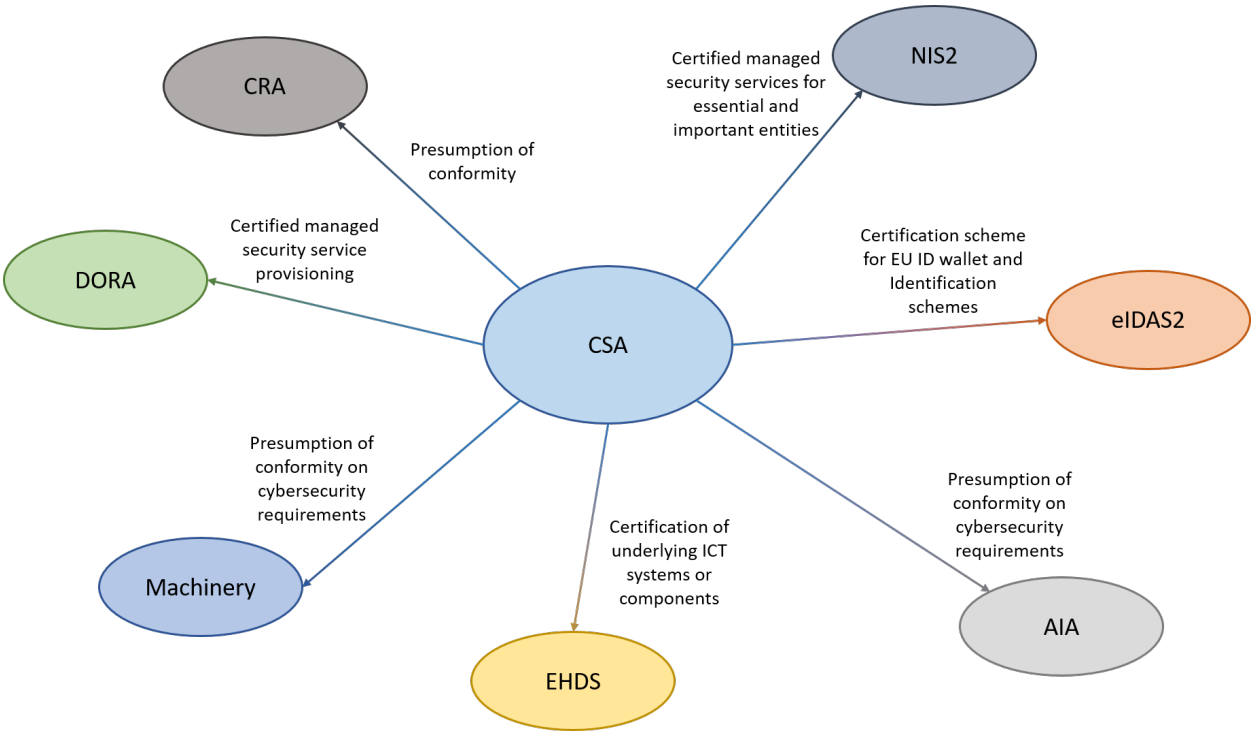
How CORAL might support this regulation

CORAL might be of direct service to this Regulation in putting into practice the content of Recital 27.

3. Conclusion

This deliverable was intended to overview the relationship between the CSA certification framework and cybersecurity requirements in the current EU regulatory landscape. In particular, it examined multiple major European regulatory frameworks, both existing and upcoming, to see how CSA certification or conformity self-assessment may allow to facilitate to comply with each such framework. A summary of the main direct findings is in the figure below.

[36] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0208
[37] EUR-Lex - 52022PC0197 - EN - EUR-Lex (europa.eu)
[38] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197



As the primary objective of CORAL project is to elaborate a toolkit and methodology to support the certification process in line with EU Cybersecurity Act in what concerns the self-certification and the basic level of assurance, this deliverable also indicates where CORAL's tools and methodology could be potentially useful in each of these frameworks.