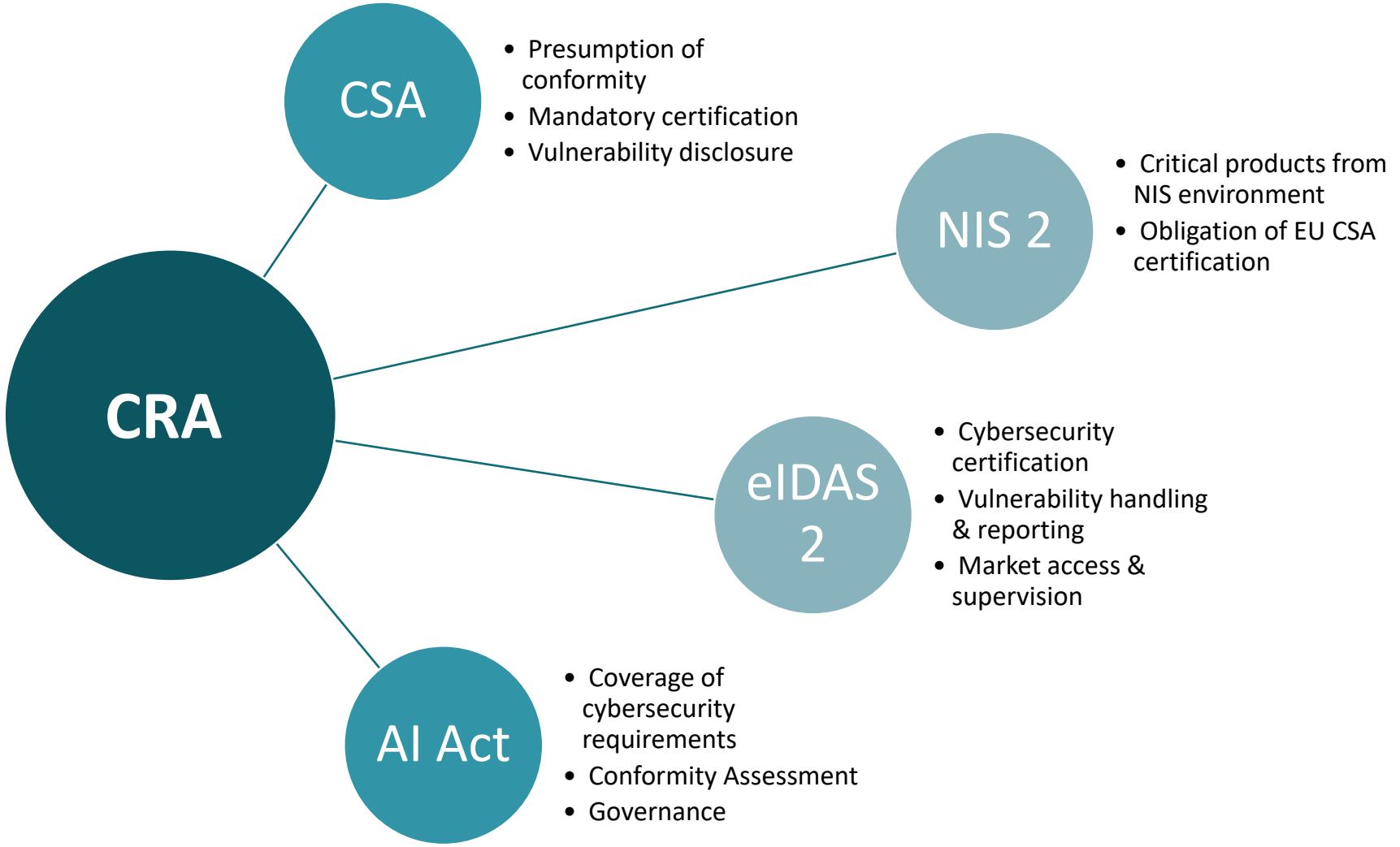
EUROSMART
The Voice of the Digital Security Industry

CRA's interplay with EU legislations referring to EU's cybersecurity certification

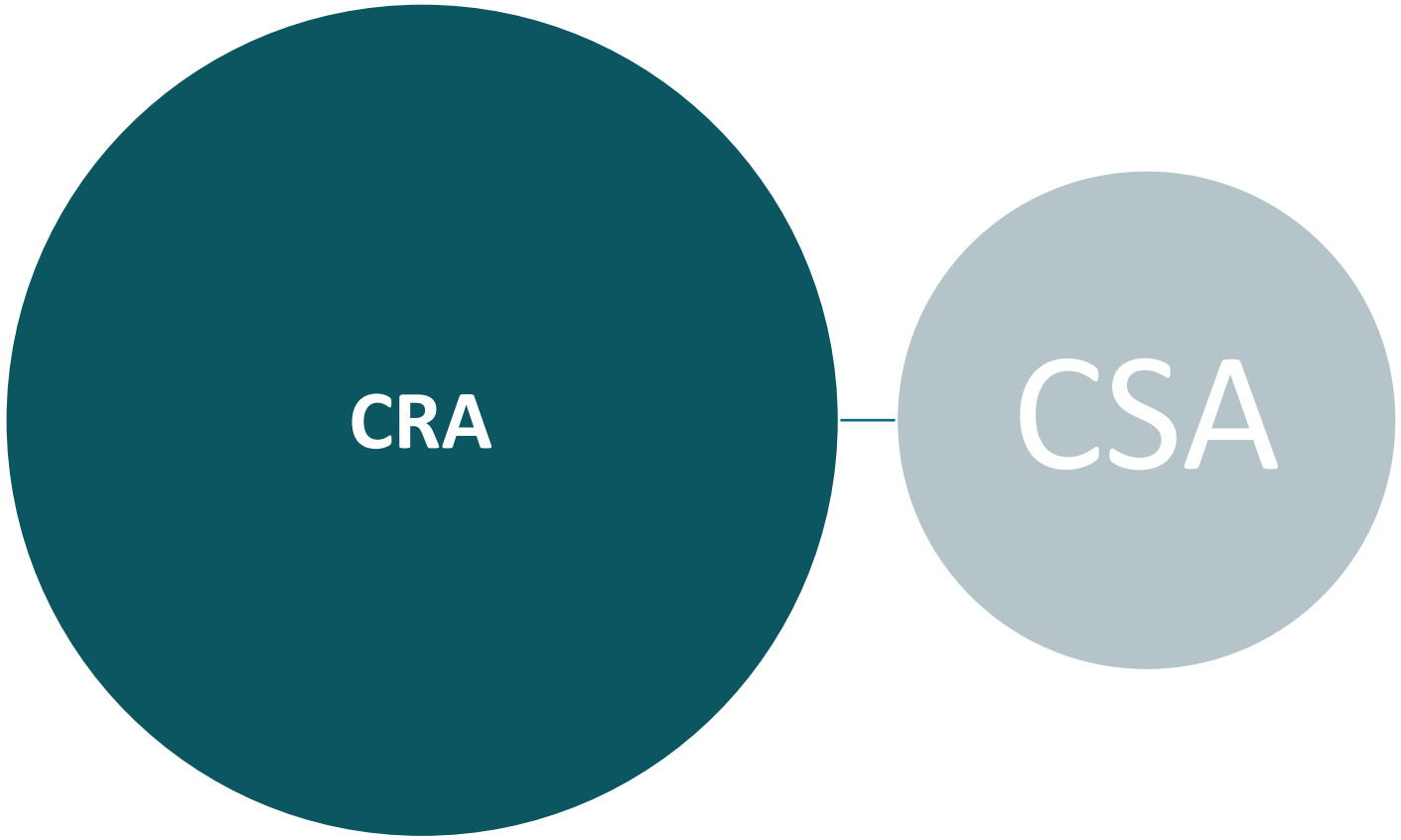
Alban FERAUD
Pierre-Jean VERRANDO

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



EUROSMART
The Voice of the Digital Security Industry

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



- Presumption of conformity
- Mandatory certification
- Vulnerability disclosure

CRA's impact on the CSA's EU cybersecurity certification framework

CSA

Reuse CSA certification to demonstrate conformity with CRA requiements – all Product classes

CSA schemes to provide **"presumption of conformity"** [art. 18.4]

- Implementing act to identify EU certification schemes (certificate + EU statement of conformity) to demonstrate conformity CRA's essential requirements
- **Could** eliminate the obligation to carry-out a third-party conformity assessment.

EU cybersecurity scheme not fully matching the CRA requirements would require the manufacturer to undergo an additional (3rd party) assessment for the elements not covered under the CRA to be able to enter the market (T2M issue)

Deserve an explicit governance to map the eligible schemes and to ensure a sufficient maintenance with regards to CRA's requirements

CRA's impact on the CSA's EU cybersecurity certification framework

Obligation to use a CSA scheme for highly critical products

Highly critical products: Conformity assessment procedure is referring to CSA certificates [art 6.5]

- Delegated acts to specify categories of highly critical products for which an EU CSA certificate is mandatory (remark: CSA declaration of conformity discarded by the legislator).
  - No CSA level defined, but the Commission to consider the level of cybersecurity risk whether the product is:
    - Used or relied upon essential entities (annex 1 of NIS2)
    - Relevant for the resilience of the overall supply chain.

CSA

This would imply the development of several vertical and/or horizontal certification schemes.
Necessary composition: Certification of processes (Annex I.2)
If rely on EUCC need for PPs developments (horizontal or sectorial) and related update to cover all the CRA's requirements.

Deserve an explicit governance:

- To identify the future "highly critical products"
- When a product is categorised as highly critical, make sure schemes, evaluation methodologies and applicable standards are developed in parallel.

CRA's impact on the CSA's EU cybersecurity certification framework

CSA

Type of conformity assessment	Class 0 "Products with digital elements"	Class I "Critical product with digital elements"	Class II "Critical product with digital elements"	Highly critical product with digital elements
Conformity to essential requirements of annex I	✓ Presumed when hEN, common specifications, EU schemes are used (art.18) if not to be demonstrated in course of conformity assessment			
Internal control procedure (based on Module A)	✓ Possible (art.24.1) easiest	✓ ⚠ *If full application of hEN, common spec, EU schemes*	✗	✗
EU-type examination procedure (based on module B) set out in Annex VI followed by ***conformity to EU-type based on internal production control*** (based on module C)	✓ Possible (art.24.1)	✓ Possible (art. 24.2)	✓ (art. 24.3)	✗
Conformity assessment based on full quality assurance (based on module H)	✓ Possible (art 24.1)	✓ Possible (art. 24.2)	✓ (art. 24.3)	✗
(EU) 2019/881 ***EU statement of conformity – Self Assessment*** [Basic CSA art.53] or ***certificate issued by a CAB or NCCA*** [Basic, Substantial and High CSA art.60]	✓ Presumption of conformity (Art.18.2) Certificate or EU statement of conformity	✓ Presumption of conformity (Art.18.2) Certificate or EU statement of conformity	✓ Presumption of conformity (Art.18.2) Certificate or EU statement of conformity	✓ European cybersecurity certificate [basic to high] (Art 6.5)

CSA Schemes to provide presumption of conformity - does not automatically eliminate the obligation of CRA's third party assessment

CSA certificates as conformity assessment by default

EUROSMART
The Voice of the Digital Security Industry

CRA's impact on the CSA's EU cybersecurity certification framework

CSA

CRA's vulnerability management

Focus on obligations to manufacturers

- [Annex I 1.2] Place on the market products without known-vulnerabilities
- [Art. 10(6)] appropriate policies and procedures, including coordinated vulnerability disclosure policies to process and remediate potential vulnerabilities in the product
- [Art. 11(1)] notify to ENISA any **actively** exploited vulnerability within 24 hours of becoming aware of it. Including where applicable, any corrective or mitigating measures - [Annex I 2.2] including by providing security updates.

- Certification schemes contain their own vulnerability disclosure and remediation measures. Risk of misalignment.
- To ensure consistency with CSA schemes a definition of "exploitable" should be included, considering the meaning of an "exploitable" vulnerability in the context of (1) the foreseen usage and (2) the risk assessment.

CRA's impact on the CSA's EU cybersecurity certification framework

CSA

EU Council perspective

Reuse CSA certification to demonstrate conformity with CRA requirements – all Product classes

The Commission to identify EU certification schemes which provide presumption of conformity with the CRA

- **Including the related conformity assessment procedures**
    - **To specify for which assurance levels the identified** schemes exempt from the **obligation to carry out third-part assessment under the CRA.**

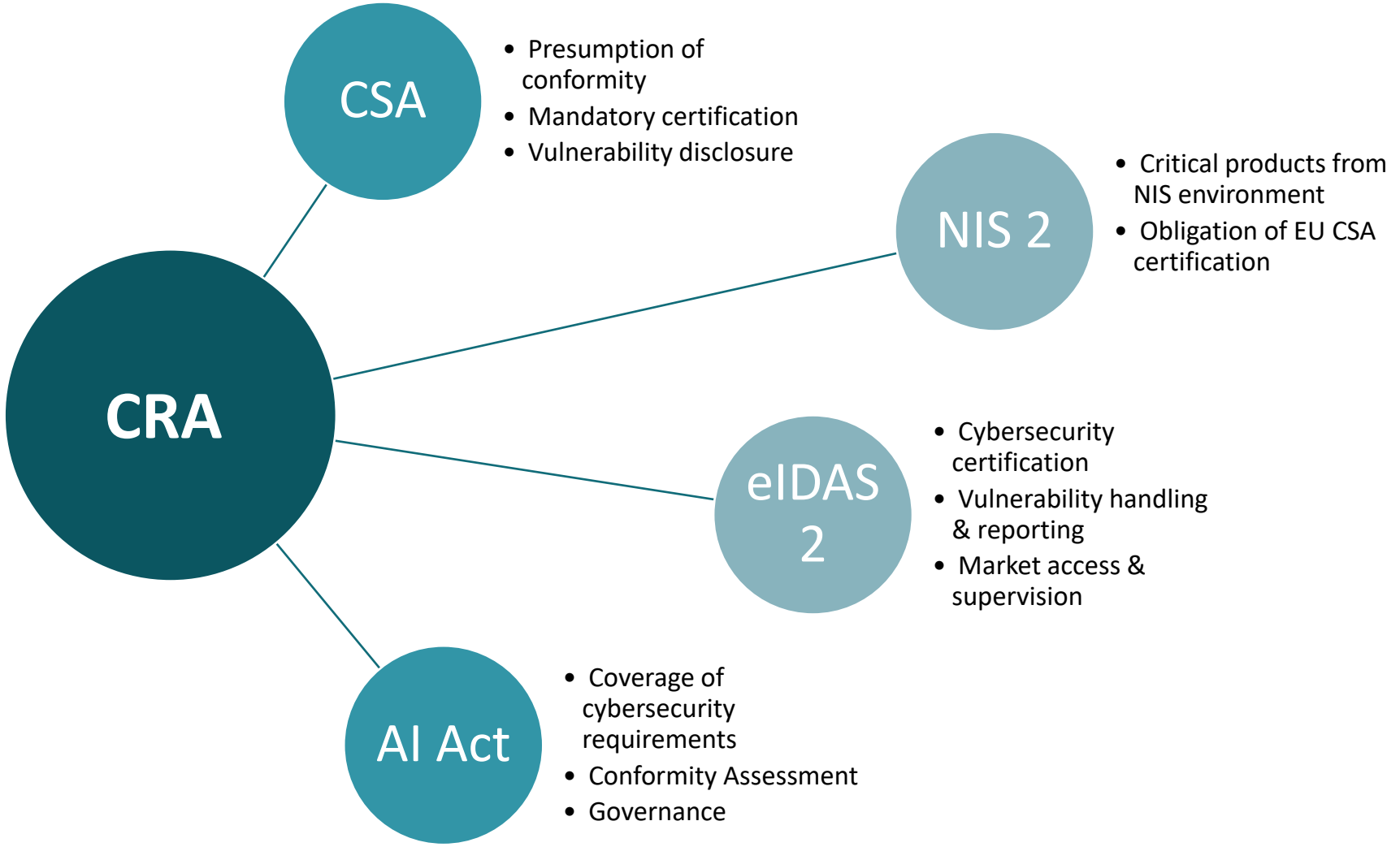
Obligation to use a CSA scheme for highly critical products

Highly critical products for which EU cybersecurity certificates are mandatory, are identify by the Commission shall fall under the (new) definition of critical products

- **Obligation to obtain « high » or « substantial » certificates**

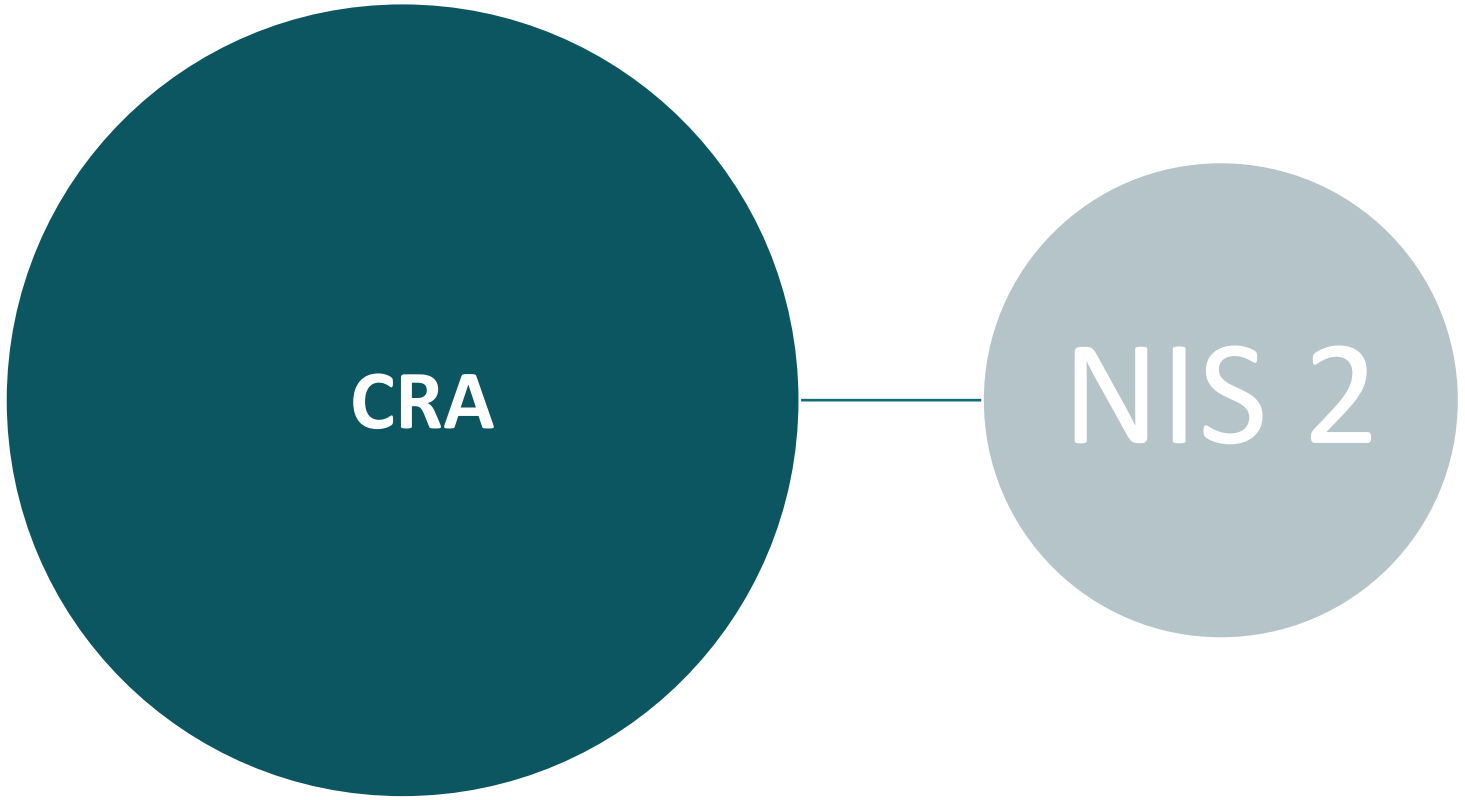
More legal certainty when it comes to the identification of the highly critical products
Governance is still missing

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



EUROSMART
The Voice of the Digital Security Industry

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



- Critical products from NIS environment
- Obligation of EU CSA certification

CRA and NIS' impact on the EU Cybersecurity certification framework

NIS 2

CRA Critical products relying on NIS environment

When listing the products falling under class I and II of annex III, one of the cretaria is:

- [art. 6(2)(b)] the intended use in sensitive environments, including in industrial settings or by essential entities of the type referred to in the Annex I to the Directive NIS 2

CRA Highly critical products with mandatory EU cybersecurity certification relying on NIS environment

When identifying the critical products, the Commission is to refer to NIS 2:

- [art. 6(5)(a)] used or relied upon by the essential entities of the type referred to in Annex I to the Directive NIS2 or will have potential future significance for the activities of these entities.

For Class I and class II, the manufacturer shall anticipate the "market"

- *[blue guide] Intended use means the use for which a product is intended in accordance with the information provided by the manufacturer (or importer) placing it on the market, or the ordinary use as determined by the design and construction of the product.*

Risk of overlap between Cloud services (NIS) and remote data processing (CRA)

- CRA more oriented towards apps on cloud

CRA and NIS' impact on the EU Cybersecurity certification framework

NIS 2

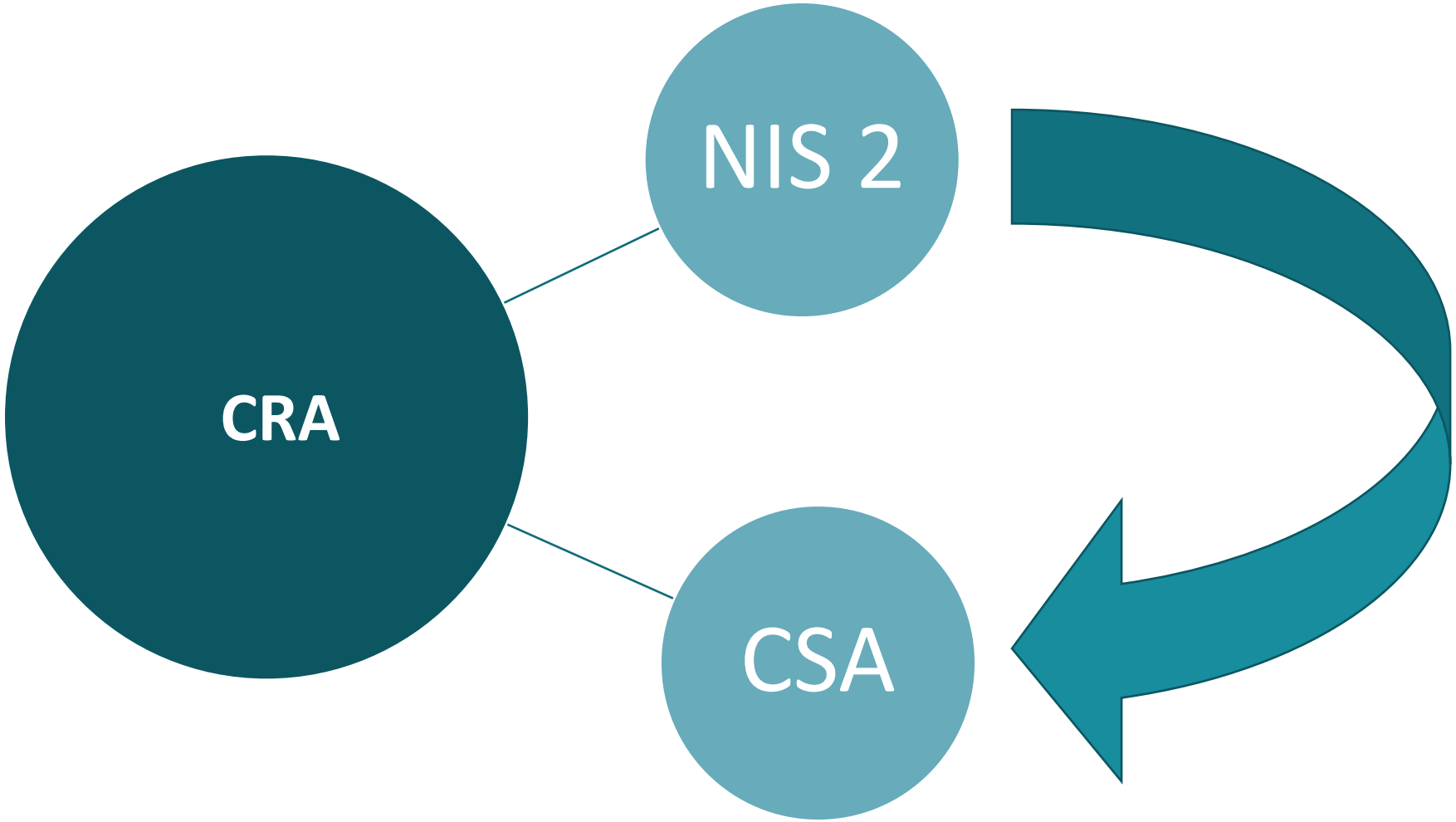
NIS' use of EU cybersecurity certification schemes

- [art. 24(1)] to demonstrate compliance with requirements of art.21 Member States may require important entities to use particular ICT products, services and processes developed by important entities that are certified under a CSA scheme.
- [art. 24(1)] The Commission to adopt delegated acts to identify which categories of essential and important entities to be required to use certain certified ICT product, processes, services.

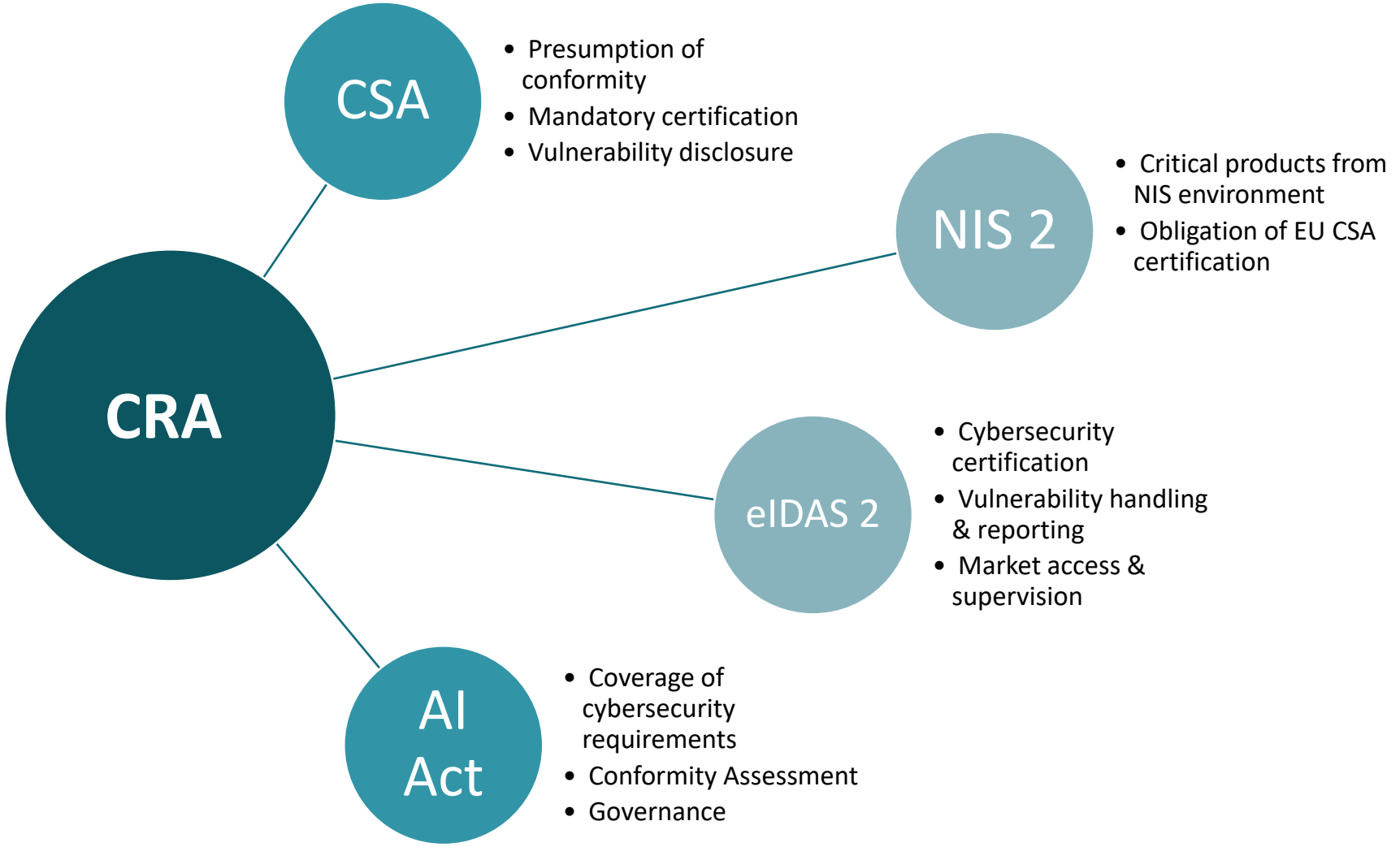
NIS more tailored for services and processes, but could target ICT products as well

- risk of overlap with CRA requirements for critical products
- Duplication of third-party assessments or certification including overlapping requirements.

CRA and NIS' impact on the EU Cybersecurity certification framework



CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



EUROSMART
The Voice of the Digital Security Industry

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification

- Cybersecurity certification
- Vulnerability handling & reporting
- Market access & supervision

CRA vs eIDAS

Different scope

- **CRA** : horizontal regulation applying to any products with digital elements
- **eIDAS** : vertical/sectorial regulation ruling its products with digital elements

eIDAS 2

eIDAS introduces three types of product with digital elements:

- Components of **Electronic identification schemes** (e.g. eID means..)
- **Wallet**
- **Qualified Signature Creation Device** (QSCD)

eIDAS also directly addresses some of the following aspects:

- **Cybersecurity certification**
- **Vulnerability handling & reporting**
- **Market access & supervision**

Main differences between CRA and eIDAS regarding cybersecurity of products with digital elements

- **CRA** : subjects of law are manufacturers/importers/distributors of products with digital elements
- **eIDAS** : subjects of law are operators of products with digital elements acting under supervision of MS

CRA vs eIDAS – cybersecurity certification

eIDAS 2

eID schemes

Article 12a (GA from the council)

- General principle of cybersecurity certification of eID scheme under relevant cybersecurity scheme pursuant to CSA. Peer review is the exception
- Cybersecurity certification shall demonstrate conformity with the requirements enacted in the LoA definition
- Entail cybersecurity certification of each of its components (eID means,..)
- Cybersecurity certification by an accredited CAB designated in accordance with regulation 765/2008

Wallet

Article 6c (GA from the council)

- Mandatory certification of Wallet to demonstrate conformity with interoperability, specific data protection and cybersecurity requirements as defined in article 6a
- Certification and cybersecurity certification shall be carried out by an accredited CAB pursuant to article 60 of CSA
- Cybersecurity certification shall demonstrate conformity with the cybersecurity requirements enacted in article 6a
- Cybersecurity certification by an accredited CAB pursuant to article 60 of CSA
- Specifications for the designation of the CAB as well as evaluation method they use to be defined

QSCD

Article 30

- Mandatory security evaluation (article 30.3)
- Cybersecurity certification shall demonstrate conformity with the cybersecurity requirements enacted in Annex II
- For local QSCD, cybersecurity certification hints toward EU CC
- For remote QSCD, no particular cybersecurity scheme is mandated

CRA vs eIDAS – cybersecurity certification

eIDAS 2

Open issues regarding the CRA

- Unlike the CRA, these cybersecurity certifications do not include general data protection requirements (e.g. definition of processing, security of processing, data minimization, integrity,..). However, these products with digital elements are used under the supervision of a **well identified controller**, which is responsible for the data processing, and to which the RGPD applies, ensuring fulfillment of all data protection requirements.

- Are the essential requirements defined in Annex I.1 all covered by the cybersecurity certification (LoA, Article 6a, Annex II)?

- How to ensure that specific products used within eIDAS context e.g. wallet or QSCD (which is a product with digital element) also meet the requirements of the CRA. Duplication of work shall be avoided. eIDAS => CRA.

- How to ensure that a product with digital elements, where reused in an eIDAS context, can be demonstrated to comply with eIDAS requirements (e.g. generic PKI; software, secure elements used within a eID scheme) . Duplication of work shall be avoided. CRA => eIDAS.

CRA vs eIDAS – vulnerability handling & reporting

eIDAS 2

eID schemes

Article 12a (GA from the council)
- Validity of cybersecurity certification set to 5 years, conditional to a regular 2 years vulnerability assessment
- Cancellation of cybersecurity certification when vulnerability has not been remediated within 3 months

Article 12
- Organize exchange of information about security breach with MS and ENISA within cooperation group

Wallet

Article 6c (GA from the council)
- Validity of cybersecurity certification set to 5 years, conditional to a regular 2 years vulnerability assessment
- Cancellation of cybersecurity certification when vulnerability has not been remediated within 3 months

Article 6d & 6da (GA from the council)
- Up to date list of certified wallet:
  - Notification of certificate of wallet being used
  - Notification when a certificate is cancelled
- Obligation of notification in case of security breach for wallet issuer/MS
- Obligation to inform users and RP in case of security breach and when it is remediated

Article 12
- Organize exchange of information about security breach with MS and ENISA within cooperation group

QSCD

Article 30
- Validity of QSCD certification set to 5 years, conditional to a regular 2 years vulnerability assessment
- Cancellation of QSCD certification when vulnerability has not been remediated

Article 31
- Up to date list of certified QSCD:
  - Notification of certified QSCD
  - Notification within one month when a certificate is cancelled

Article 17
- Organize exchange of information about security breach with other supervisory bodies
- Obligation of information to the public

Article 19
- Obligation of notification of security breach for QTSP (using QSCD)
- 24h for notifying supervisory bodies & competent authorities
- Obligation to inform natural/legal persons of the security breach
- In case where several MS are impacted, supervisory body shall inform the other supervisory bodies and ENISA

CRA vs eIDAS – vulnerability handling & reporting

eIDAS 2

Mapping and alignment between the eIDAS and (1) essential requirements defined in Annex I.2 (vulnerability handling) and (2) article 11 of the CRA is needed.

- Regular 2 years vulnerabilities assessment (Annex I.2(3)) => A comprehensive mapping of Annex I.2 is needed
- Exchange of information on security breaches between authorities => Overlap with article 11 of the CRA but different governance (ENISA => CyCLONe vs ad hoc structure)
- Obligation of information to users and Relying party (Wallet) or the public (QSCD) => Overlap with article 11 of the CRA, but broader scope
- Obligation of vulnerability reporting for QSCD through QTSP supervision => Overlap with article 11 of the CRA but different implementation : governance (MS PoC vs ENISA) & different subject of law with different delay (24h for QTSP vs 24h for the manufacturer of the product with digital element)

eIDAS defines supplemental mechanisms that may also be of interest for the CRA

- Up to date list of certified products (Wallet, QSCD) where the CRA only provides for communication where a product is withdrawn or recalled
- Rules for certification cancellation which are missing under the CRA

CRA vs eIDAS – market access & supervision

eIDAS 2

eID schemes

Article 12a (GA from the council)

- Where certification of a component is lost, it can't be used anymore

Wallet

Article 6c (GA from the council)

- Where certification is lost, it can't be used anymore

Article 6da (GA from the council)

- In case of security breach, issuance and use of the wallet shall be suspended
- Where the security breach is remediated, issuance and use of the wallet shall be re-established
- Where the security breach is not remediated within 3 month, or if it is justified by its severity, the wallet shall be withdrawn without undue delay

QSCD

Article 30

- Cancellation of QSCD certification when vulnerability has not been remediated

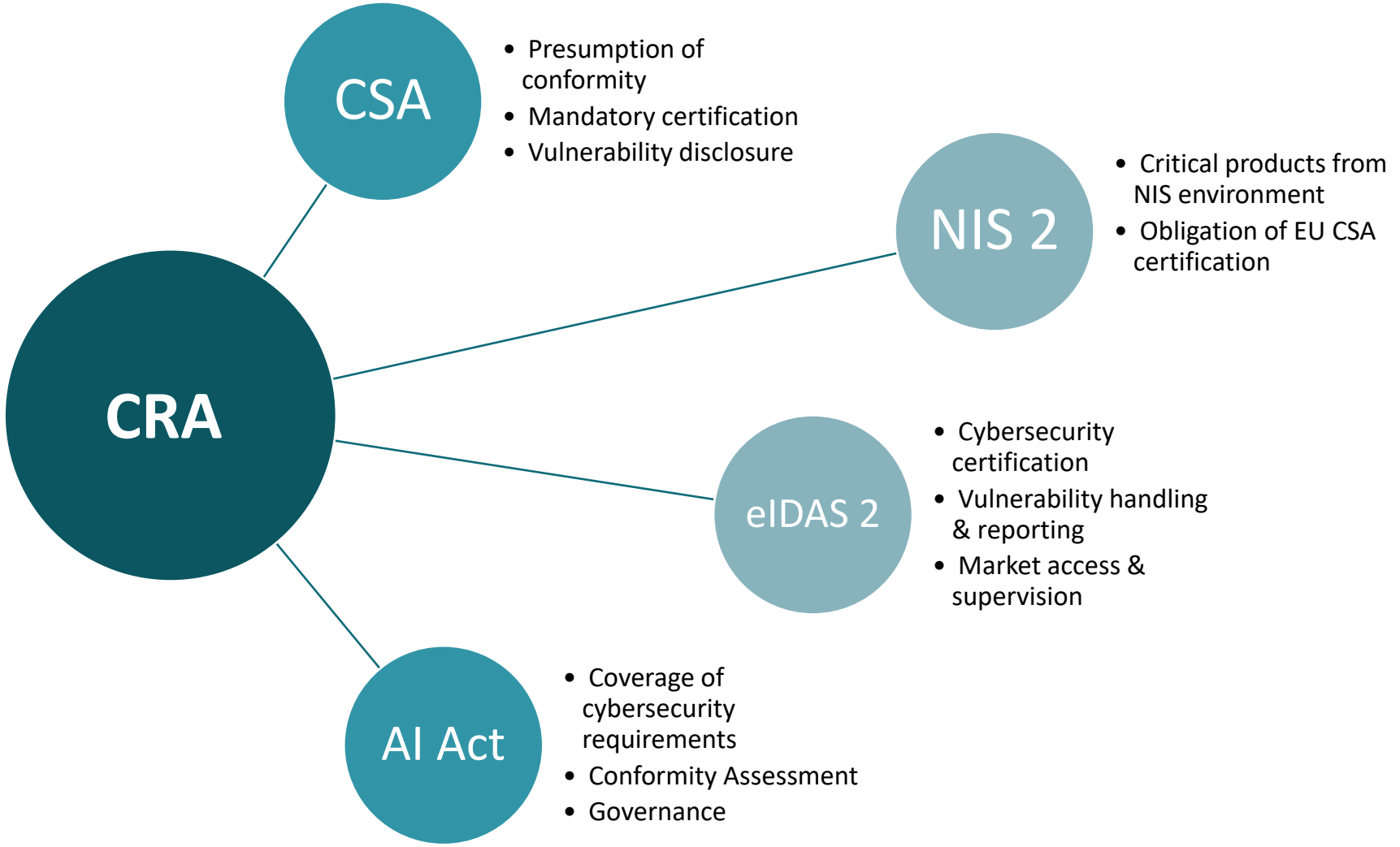
Article 25

- Loss of QSCD certificate implies loss of legal value of any future electronic signature created. QTSP can't use them anymore and have to replace them.

eIDAS contains its own market access rules for its product with digital elements

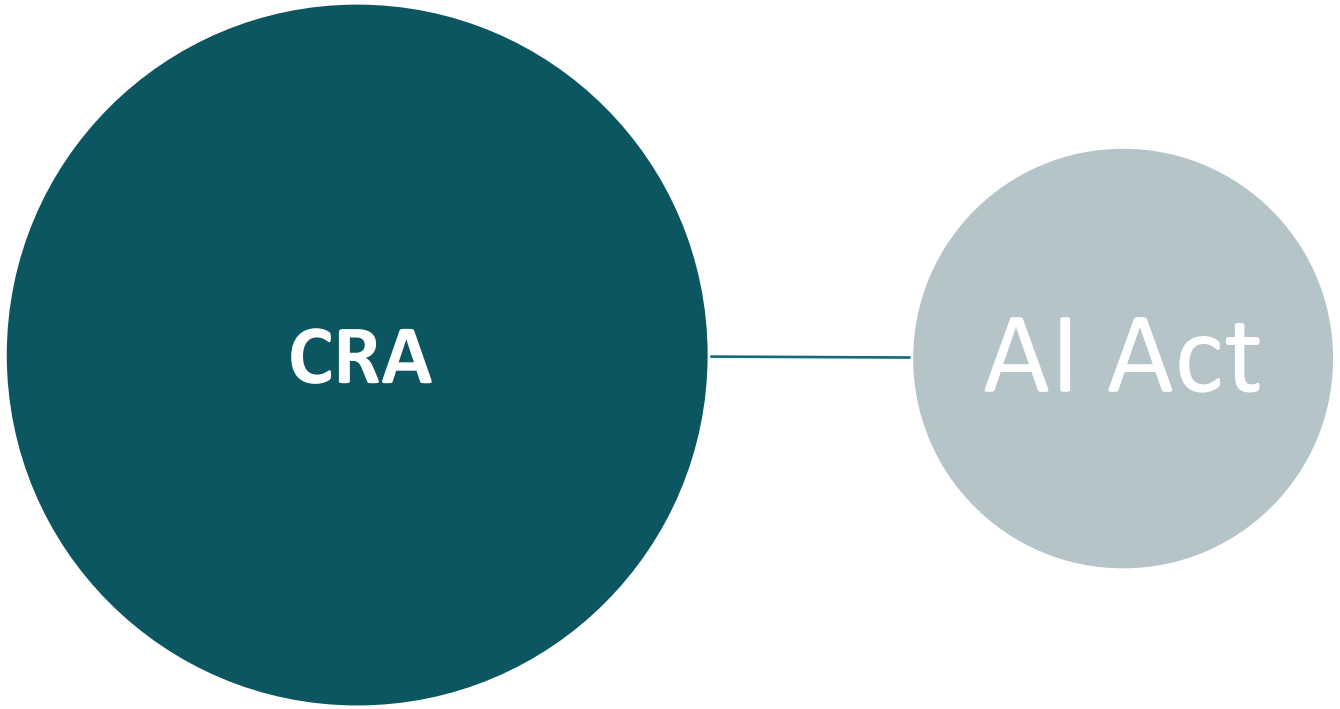
- Certification NOK => Withdrawal of the product from the market
- Market access may be restored if the product is fixed so that the certification is restored (e.g. when the product receives a security patch)
- BUT market supervision governance is already ensured by bodies which are different from the ones defined in the CRA

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



EUROSMART
The Voice of the Digital Security Industry

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



- Coverage of cybersecurity requirements
- Conformity Assessment
- Governance

CRA vs AI Act

AI Act

Any AI-system may fall into the scope of the CRA

- BUT High-risk AI-system are subject to specific market access supervision as defined in AI Act, which also list their cybersecurity as an essential requirement
- To avoid double conformity work regarding cybersecurity requirements, CRA defines specific handling for high-risk AI system (article 8)
- Where the essential requirements of Annex I of the CRA are fulfilled, the high-risk AI-system is presumed in compliance with the cybersecurity requirements set out in article 15 of AI Act.

Open issues

- Coverage of cybersecurity requirements
- Conformity assessment
- Governance

CRA vs AI Act - Coverage of cybersecurity requirements

AI Act

RGPD will apply for high-risk AI systems to cover both the processing of personal data during training and usage

General data protection requirements (e.g. security of processing, data minimization, integrity,..) set out in the RGPD are much more suitable than those found in Annex I of CRA as

- They are much more complete
- They acknowledge the key role of the entity in charge of training and the operator of the AI system

to secure the data processing

- The essential requirements dealing with data processing found in Annex I of CRA may create unnecessary redundancy in the course of conformity assessment.

- This is also true for any product with digital elements, where RGPD will always apply and ensure a broader coverage of data protection requirements than Annex I of CRA.

CRA vs AI Act – Conformity assessment

AI Act

- For critical (some types) and non-critical product, conformity assessment shall be carried out in accordance with AI Act
- BUT conformity assessment between AI Act and CRA are different

⚠ **It is not obvious that both conformity assessment procedure are commensurate**

- Are the level of risk of an AI system and its cybersecurity independent?
- Shouldn't the level of cybersecurity be commensurate with the level of risk of an AI system?

⚠ **If an AI-system is high-risk, shouldn't it always ensure a high level of cybersecurity to ensure human rights are guaranteed?**

CRA vs AI Act – Governance

AI Act

Cooperation between AI Act & CRA governances

For critical (some types) products, conformity assessment shall be carried out pursuant to the CR

What about cooperation regarding conformity of the high-risk AI-system?

- Carried out pursuant to AI Act
- Reused results regarding cybersecurity obtained under the CRA
- What about cooperation regarding accreditation and qualification of CAB between both domains?

Market supervisionS

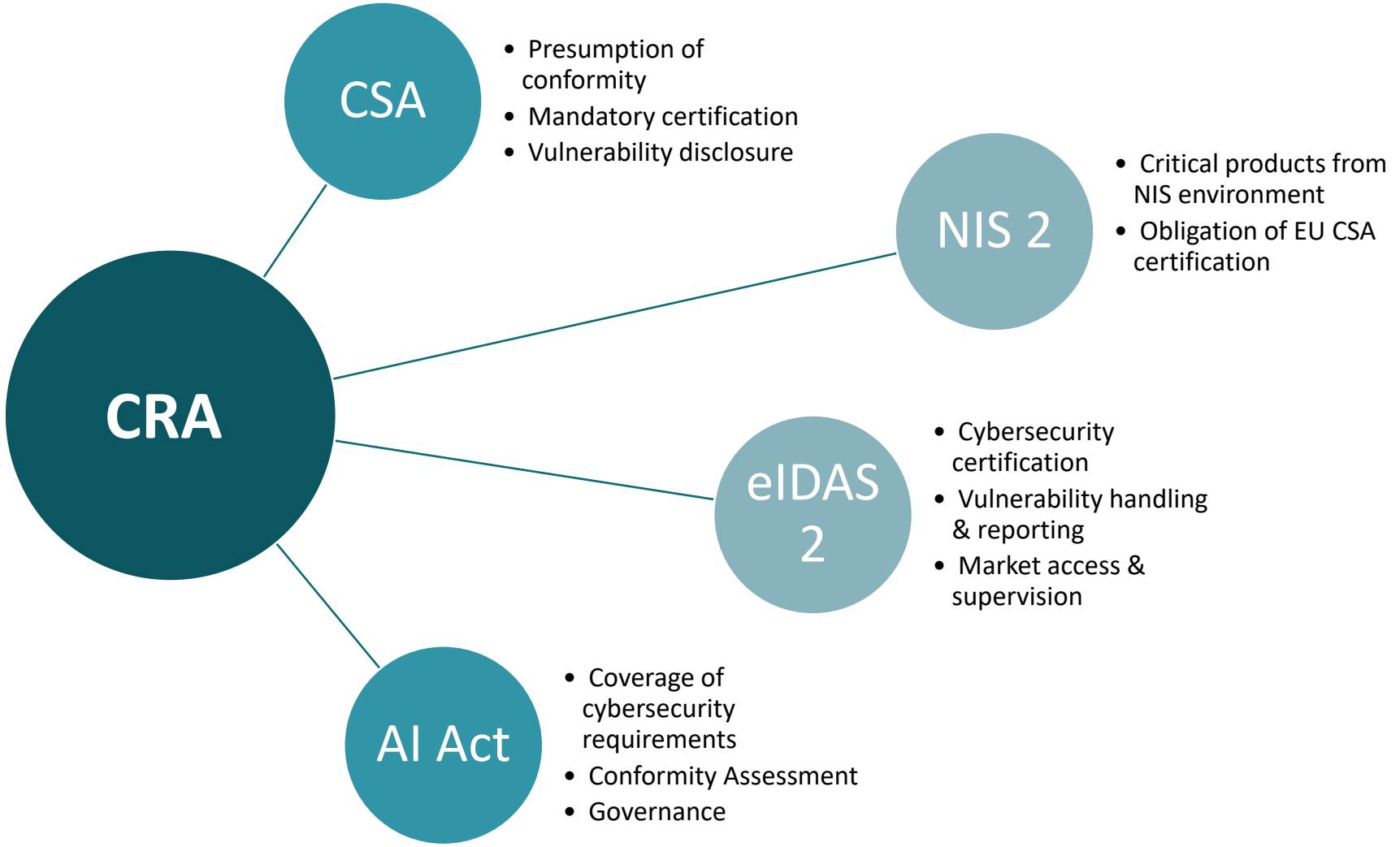
Except conformity assessment procedure, the CRA always applies to high-risk AI systems:

- obligation of reporting (article 11) with its own governance
- obligation to economic operators
- Market supervision
- Specific actors (e.g. AI Board,..)
- ...

How will it articulate with market supervision defined by the AI Act involving other actors?

Governance between both texts shall be clarified

CRA's interplay with EU legislations referring to EU's cybersecurity evaluation / certification



EUROSMART
The Voice of the Digital Security Industry

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Thank you

Eurosmart | Square de Meeûs 35 | 1000 Brussels | Belgium