Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Europese ontwikkelingen

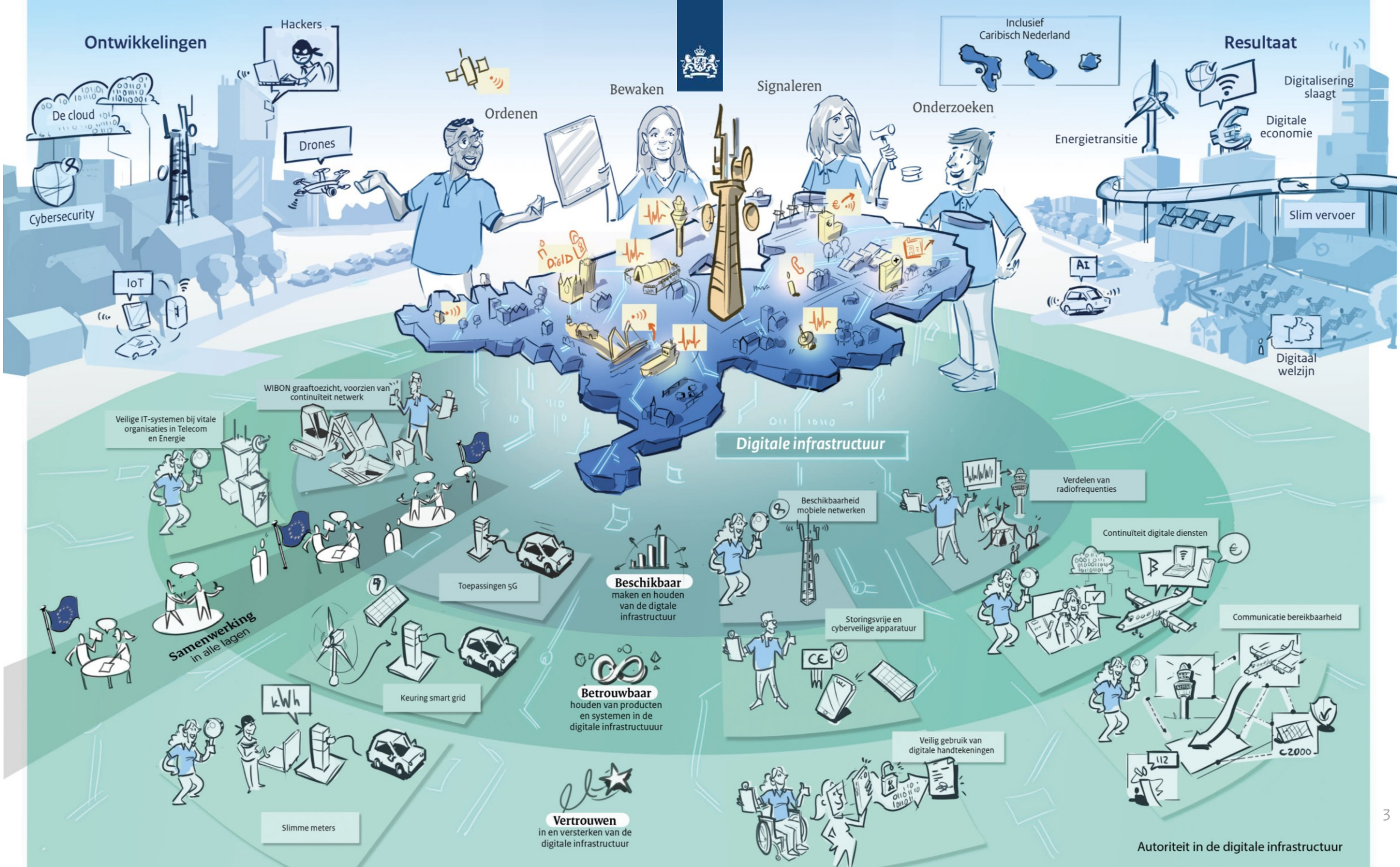
Regelgeving en cybersecurity

Voor een **veilig verbonden** Nederland

22 April 2026

Ruud Kerssens RE RA CISA CRISC

Inhoudsopgave


Ontwikkelingen
Hackers
De cloud
Drones
Cybersecurity
IoT
Ordenen
Bewaken
Signaleren
Onderzoeken
Inclusief Caribisch Nederland
Resultaat
Digitalisering slaagt
Digitale economie
Energietransitie
Slim vervoer
AI
Digitaal welzijn
WIBON graaftoezicht, voorzien van continuiteit netwerk
Veilige IT-systemen bij vitale organisaties in Telecom en Energie
Digitale infrastructuur
Verdelen van radiofrequenties
Beschikbaarheid mobiele netwerken
Continuïteit digitale diensten
Communicatie bereikbaarheid
Toepassingen 5G
Beschikbaar
maken en houden van de digtale infrastructuur
Storingsvrije en cyberveilige apparatuur
Samenwerking
in alle lagen
Keuring smart grid
Betrouwbaar
houden van producten en systemen in de digitale infrastructuuur
kWh
Slimme meters
Vertrouwen
in en versterken van de digitale infrastructuur
Veilig gebruik van digitale handtekeningen
112
C2000
Autoriteit in de digitale infrastructuur

Intro

- **Doel presentatie:**

  Inzicht in EU ontwikkelingen regelgeving en cybersecurity als referentie voor audit en advisory.

- **Gewenste uitkomst**

  Verdiep je in de regelgeving en leer van ontwikkelde standaarden, pas deze toe en overweeg een bijdrage te leveren.

- **Europees speelveld**
  - Sterk in digitalisering
  - Meer regulering en harmonisatie versus Tsunami
  - Minder afhankelijkheid
  - Verhogen van de cyberweerbaarheid
  - Digital Omnibus: efficiënter

- **Ecosystems cybersecurity:**
  - Legislation specific
  - NLF
  - CSA

1. NLF - New Legislative Framework

- EU Product regulation met inzet van standaardisatie door regelgeving
  - Regulation (EC) 765/2008 setting out the requirements for accreditation and the market surveillance of products.
  - Decision 768/2008: on a common framework for the marketing of products, which includes reference provisions to incorporate in product legislation revisions.
  - Regulation (EU) 2019/1020: on market surveillance and compliance of products.
  - ‘the Blue Guide’.

- New Legislative Framework
  - Accreditation (notified bodies)
  - Conformity assessment
  - CE marking
  - Market surveillance
  - Toolbox
- Medical / Gas / Drones / Batteries / Machinery …
- Artificial Intelligence Act - Regulation (EU) 2024/1689
- Cyber Resilience Act - Regulation (EU) 2024/2847

NLF-Cybersecurity

- Radio Equipment Directive = Directive → vergt nationale implementatie
- Cyber Resilience Act = Act → Europa effectief

"products with digital elements that are connected—either directly or indirectly—to another device or network"

2026

11 juni 2026
Hoofdstuk 4 van de CRA van kracht

30 augustus 2026
Deadline standaardisatieverzoek raamwerkstandaard

30 augustus 2026
Deadline standaardisatieverzoek horizontale standaarden

30 augustus 2026
Deadline standaardisatieverzoek verticale standaarden

11 september 2026*
Inwerkingtreding actief misbruikte kwetsbaarheden en ernstige incidenten

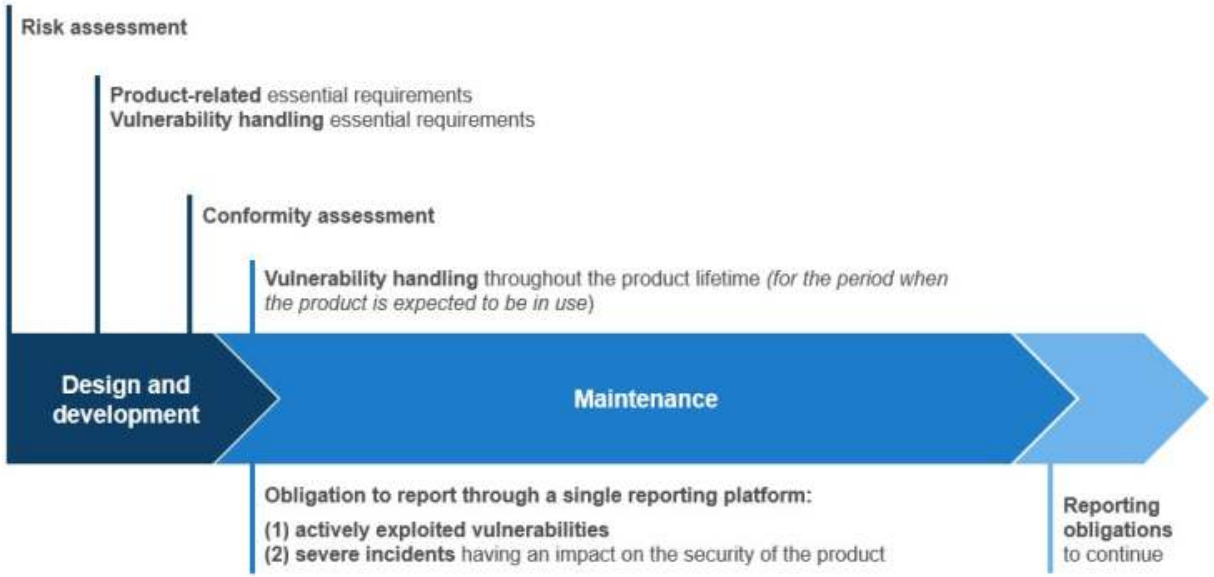
2027

30 oktober 2027
Deadline horizontale standaarden

11 december 2027
De gehele CRA is van kracht.

Onderwerpen

- Scoping
  - Default
  - Important (type I en II) (Annex III)
  - Critical (Annex IV) → link naar CSA
  - Life-cycle
- Risk assessment (what)
  - “Security by design”
  - “Secure by default”
  - “Logging and monitoring”
- Conformity assessment (how)
- Declaration of conformity
- Vulnerability handling (relatie met SBOM)
- Reporting



https://digital-strategy.ec.europa.eu/en/policies/cra-manufacturers

(Essential) Security requirements ....

Part II of Annex I. Article 13(8)

- No known vulnerabilities
- Secure configuration by default
- Security updates
- Protection against unauthorised access
- Protecting data confidentiality and data integrity
- Data minimisation
- Ensuring availability
- Limiting negative impact on other systems
- Reducing the attack surface
- Limiting the consequences of incidents
- Logging and monitoring
- Secure deletion of data

Deel II Annex I. Vereisten inzake de respons op kwetsbaarheden

Annex II: Informatie en instructie voor de gebruiker

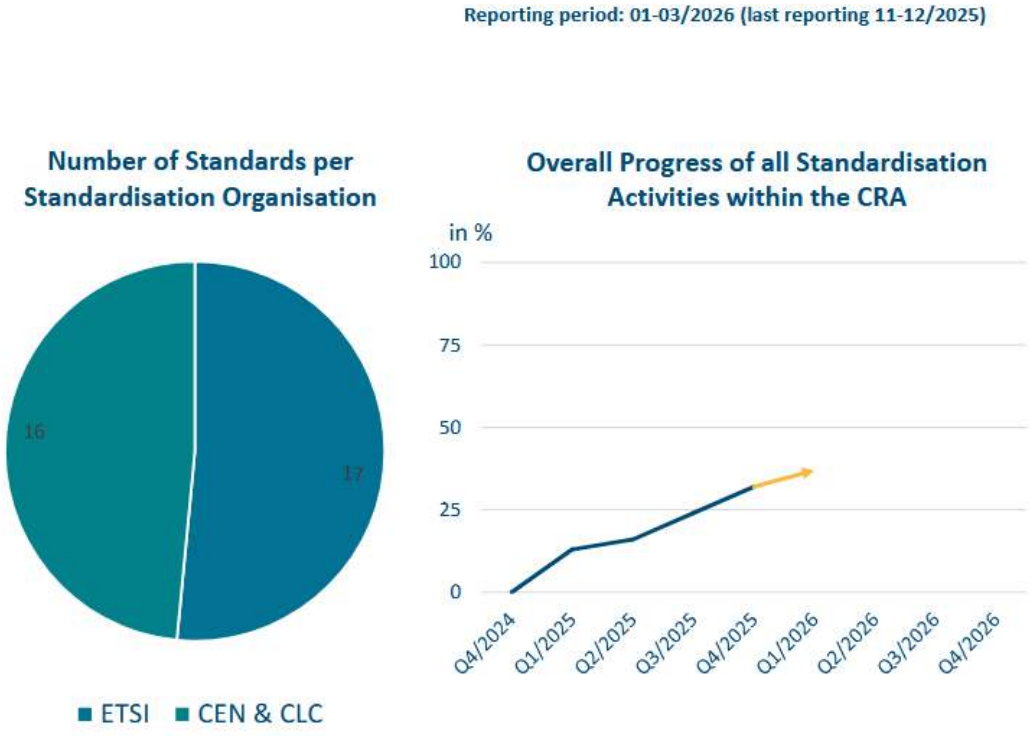
Annex VII: Inhoud technische documentatie

Annex VIII: Conformiteitsbeoordeling

Actueel

- **(EU) 2025/2392 (28/11/2025) technical description of the categories of important and critical products**
- **Draft Commission guidance on the Cyber Resilience Act**

  Feedback period 03 March 2026 - 13 April 2026 (midnight Brussels time)
- **Standards!** Normalisatieverzoek M/606, van de Commissie
- **Cyber Resilience Act Requirements Standards Mapping - Joint Research Centre & ENISA Joint Analysis** (4 April 2024)
- **Annual Union Work Programme 2026 for European Standardization (AUWP 2026)**
  - veiligheid in de EU (**actie 5 – cyberbeveiligingsvereisten voor producten met digitale elementen, actie 25 – kritieke communicatienetwerken voor openbare veiligheid en beveiliging**);
- Workshops (ETSI, CYBERSTAND.eu and STAN4CRA.eu)

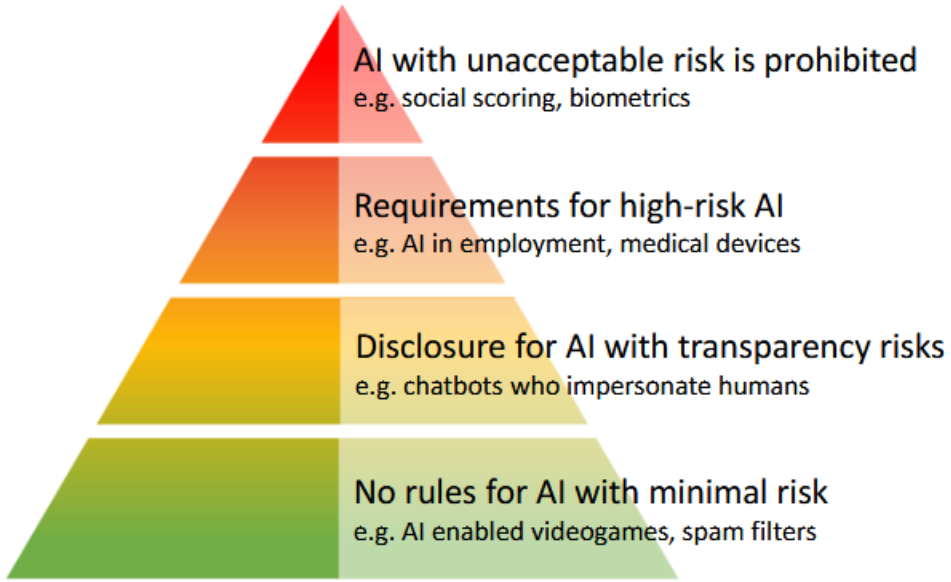


https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/CRA/Dashboard_CRA.pdf?__blob=publicationFile&v=6

NLF- Artificial Intelligence

Regulation (EU) 2024/1689

Risk-based rules for AI systems:



Risk Management	Data governance and Data Quality	Record keeping and Logging	Transparency
Human Oversight	**Accuracy**	Robustness	Cybersecurity
	Quality Management	Conformity Assessment	

Rules for AI systems (i.e. prohibitions, high-risk, transparency) → **Market surveillance authorities**

Rules for general-purpose AI models → **Commission (AI Office)**

AI Board
with EU Member States to coordinate at EU level

Scientific Panel
supports with independent technical advice

Advisory Forum
supports with stakeholder input

AIA timeline

https://artificialintelligenceact.eu/implementation-timeline/ (gedetailleerd)

02 Feb 2025 — General provisions (definitions & AI literacy) and prohibitions apply

02 Aug 2025 — Rules for general-purpose AI apply and governance must be in place

- AI Act obligations for providers of general-purpose AI models enter into application
- Member States need to designate national competent authorities and adopt national laws on penalties
- EU-level governance (AI Board, Scientific Panel, Advisory Forum) must be set up

02 Aug 2026 — The majority of rules of the AI Act come into force and enforcement starts

- Rules for high-risk AI systems in Annex III enter into application **
- Transparency rules (Article 50) start to apply
- Measures in support of innovation start apply
- Member States should have at least one AI regulatory sandbox per country established
- Enforcement of the AI Act starts at national and EU-level

02 Aug 2027 — Rules for high-risk AI embedded in regulated products apply **

https://ai-act-service-desk.ec.europa.eu/en/ai-act/timeline/timeline-implementation-eu-ai-act

AIA and cybersecurity

- Article 15: **Accuracy, Robustness and Cybersecurity**
- 5. High-risk AI systems shall be resilient against attempts by unauthorised third parties to alter their use, outputs or performance by exploiting system vulnerabilities. The technical solutions aiming to ensure the **cybersecurity** of **high-risk AI systems shall** be appropriate to the relevant circumstances and the risks. The technical solutions to address AI specific vulnerabilities shall include, where appropriate, measures to prevent, detect, respond to, resolve and control for attacks trying to manipulate the training data set (**data poisoning**), or pre-trained components used in training (**model poisoning**), inputs designed to cause the AI model to make a mistake (adversarial examples or **model evasion**), confidentiality attacks or **model flaws**.

NOW

IN_DEVELOPMENT

prEN 18282

30.99 CD approved for registration as DIS

Apr 16, 2026

AIA and cybersecurity

- Harmonised Standards request — M/613 (CEN/CENELEC JTC 21)
- Code of Practice for General-Purpose AI Models Safety and Security Chapter
- Interplay met CRA (Art. 43 AIA + Article 12-13 CRA)
- Interplay met CSA (Art. 15 and 42 AIA; Titel III CSA) - certification under applicable scheme creates a presumption of compliance with the cybersecurity requirements set out in Article 15 of the AI Act
- Standardization
  - (JTC21 CEN/CENELEC WG5) → Cybersecurity specifications for AI Systems (prEN 18282) ➔ OWASP AI Exchange relevance
  - (ETSI) ETSI ETSI TR 104 128 **TR** Guide to Cyber Security for AI Models and Systems; **EN** 304 223 Baseline Cyber Security Requirements for AI Models and Systems + ETSI **TR** 104 030 Critical Security Controls for Effective Cyber Defence; ETSI TS 104 224 **TS** Explicability and transparency of AI processing
  - ISO/IEC FDIS 27090 Cybersecurity — Artificial Intelligence — Guidance for addressing security threats and compromises to artificial intelligence systems
- Plus: Logging (prEN ISO/IEC 24970) / AI trustworthiness framework – Part 1: Logging, transparency and human oversight (prEN 18229-1) / AI trustworthiness framework – Part 2: Accuracy and robustness (prEN 18229-2) / Conformity Assessment (prEN 18285) / Risk Management (prEN 18228)

2. CSA (Cybersecurity Act) + EUCC = Common Criteria

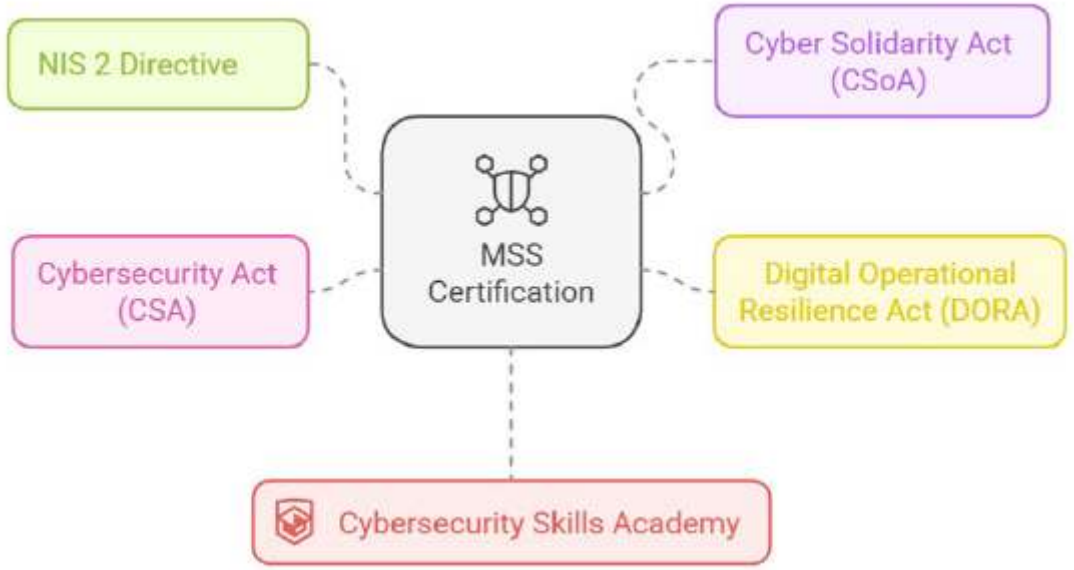
- CSA
  - Interplay met CRA (Article 8 - Critical products with digital elements)
  - Interplay met AIA (Article 42: Presumption of conformity with certain requirements; paragraph 2 for high risk systems)
- Enig schema CSA = EUCC
- Hoge verversing
  - 2023: Implementing Act
  - 2024/12 Amendment 1
  - 2025/12 Amendment 2
  - …
- Protection profiles
- SG Crypto “Agreed Cryptographic Mechanisms”
- SOTA (State-of-the-Art)
- Rol in EUDI Wallet

CSA - EUCS = Cloud services

- Schema maart 2024…
- CEN TS 18026 (2024) requirements / CEN TS 18072 (2025) assessment methodology
- Pauze, Pending CSA2
- FAQ CSA 2:
  - *the work related to the schemes for cloud services (EUCS) and 5G (EU5G) is expected to resume.*
  - *On cloud, the new Cybersecurity Act complemented by the upcoming CADA will fill gaps related to sovereignty aspects and non-technical risks*

CSA – EUMSS = Managed Security Services

- Cybersecurity certificatieschema Managed Security Services
- Afgeleide van de Cybersolidarity Act (link naar ook Cyber Reserve)
- Link naar NIS2 (EU) 2024/2690 of 17 October 2024: *Implementing regulation 2024 voor Digital Service Provides* for application of Directive (EU) 2022/2555 (NIS2)
- AdHoc Working Group met Nederlandse inbreng!
- Eind 2026 Implementing Regulation en starten met accreditatie / autorisatie!
- Service profile “Incident response”. Daarna …..



CSA - EUDI Wallet (e-IDAS2)

- Doel:
  - Secure identification and authentication
  - Exchanging qualified and non-qualified User attributes
  - Electronic signing of documents or data
  - Generate and use pseudonyms
- Nationaal schema eerst (??)
- Parallel certificatieschema EUDI Wallet
- EUDI Wallet Architecture and Reference Framework (ARF)
- Interplay CRA en EUCC

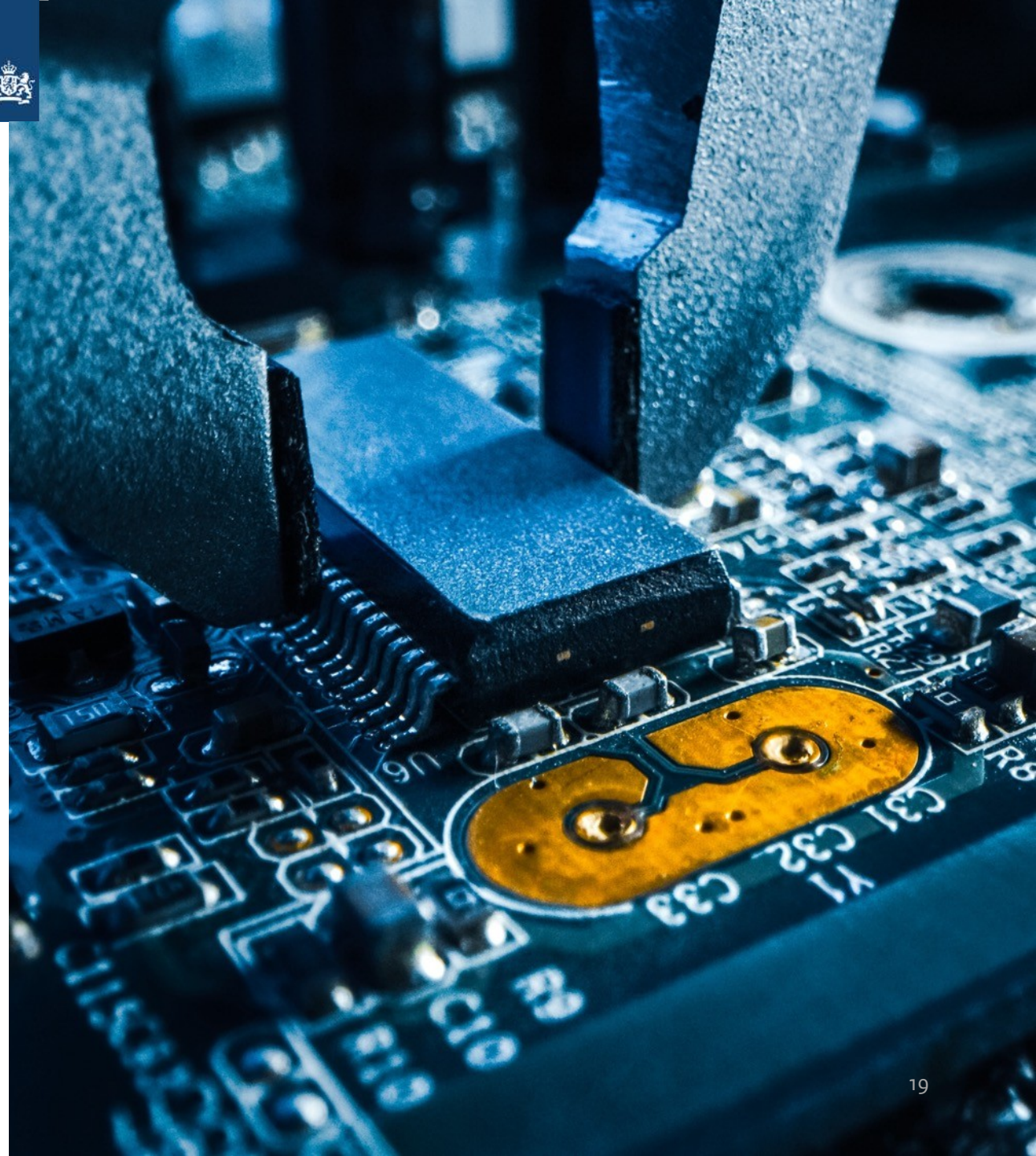
CSA - CEN TS 18072

Assessment methodologie:

- Origin: Requirements for Conformity Assessment Bodies certifying Cloud Services
- Requirements for conformity assessment bodies certifying ICT services
- AddOn op ISO/IEC 17065 Conformity assessment — Requirements for bodies certifying products, processes and services
- NL inbreng met Meta-approach
- Alignen ISAE met Certificatie vraagt ook aandacht in (IT) audit wereld
- Certificering = nieuwe aspecten

3. CSA 2

- Titel 1: Introductie “Cyber posture”;
- Titel 2: Rol ENISA / EC – grotere scope, minder invloed lidstaten, **standaarden**, vergoedingen /ECSF
- Titel 3: Correcties CSA 1 uitwerking Cyber posture / Technische schema’s / minder invloed lidstaten
- Titel 4: Security of supply chains, bepalende rol EC, sancties voor high risks suppliers



Amendments NIS2

amending Directive (EU) 2022/2555 as regards simplification measures and alignment with the [Proposal for the Cybersecurity Act 2]

- Aanpassingen Annex I van de NIS2, dus scope
  - Entiteiten betrokken bij EUDI Wallet / EU Business wallet
  - Introductie “small mid-cap” → van essentieel naar belangrijk → lichter toezichtsregime
- Alignment met “cyber posture” certificering voor “presumption of conformity”
- Post Quantum
- Ransomware

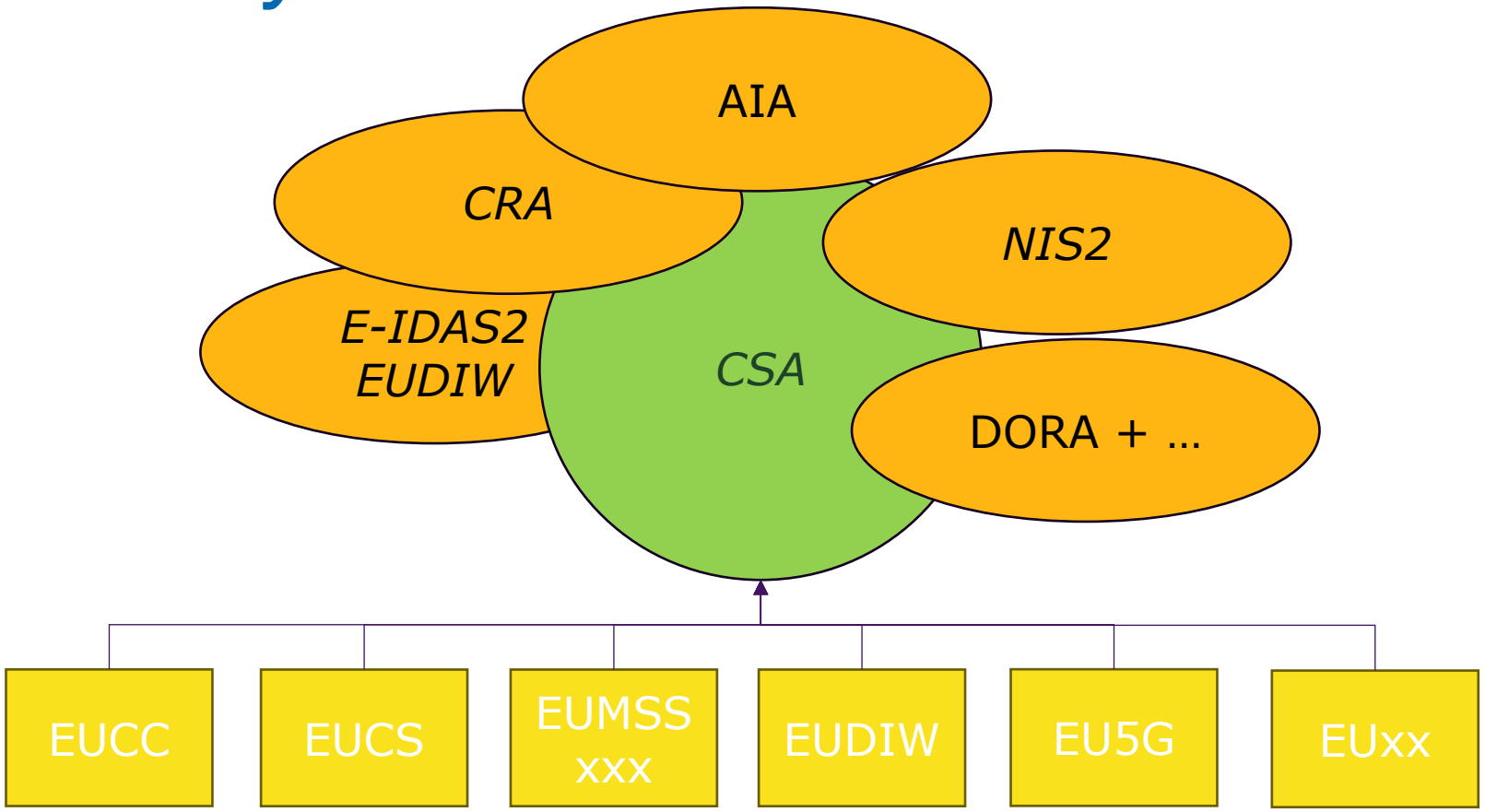
Security of supply chains

- Art. 100 - Designation of third countries "posing cybersecurity concerns"
- High risk suppliers
- Risk assessment
  - Cyber threat - ICT supply chain
  - Identification key ICT assets
  - Mitigation in ICT supply chain
  - Identification of high-risk suppliers

  (Located in 3rd country posing cybersecurity concerns)

- Sancties
  - Geen betrokkenheid standaarden / common specifications
  - Geen CSA certificering
  - Geen accreditatie
  - Geen public procurement deelname
  - Geen EU fondsengebruik

Cybersecurity - summary



Zijn er nog vragen?

Voor een **veilig verbonden** Nederland

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Contact

088 041 60 00 info@rdi.nl www.rdi.nl

Social Media

#wijzijnRDI