Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

CSA Services schemes

Voor een **veilig verbonden** Nederland

Agenda

1. NCCA Activities ICT Services
2. Standards CEN TS 18026 and 18072
3. EUMSS – Candidate scheme status
4. Revision CSA (2019/881)

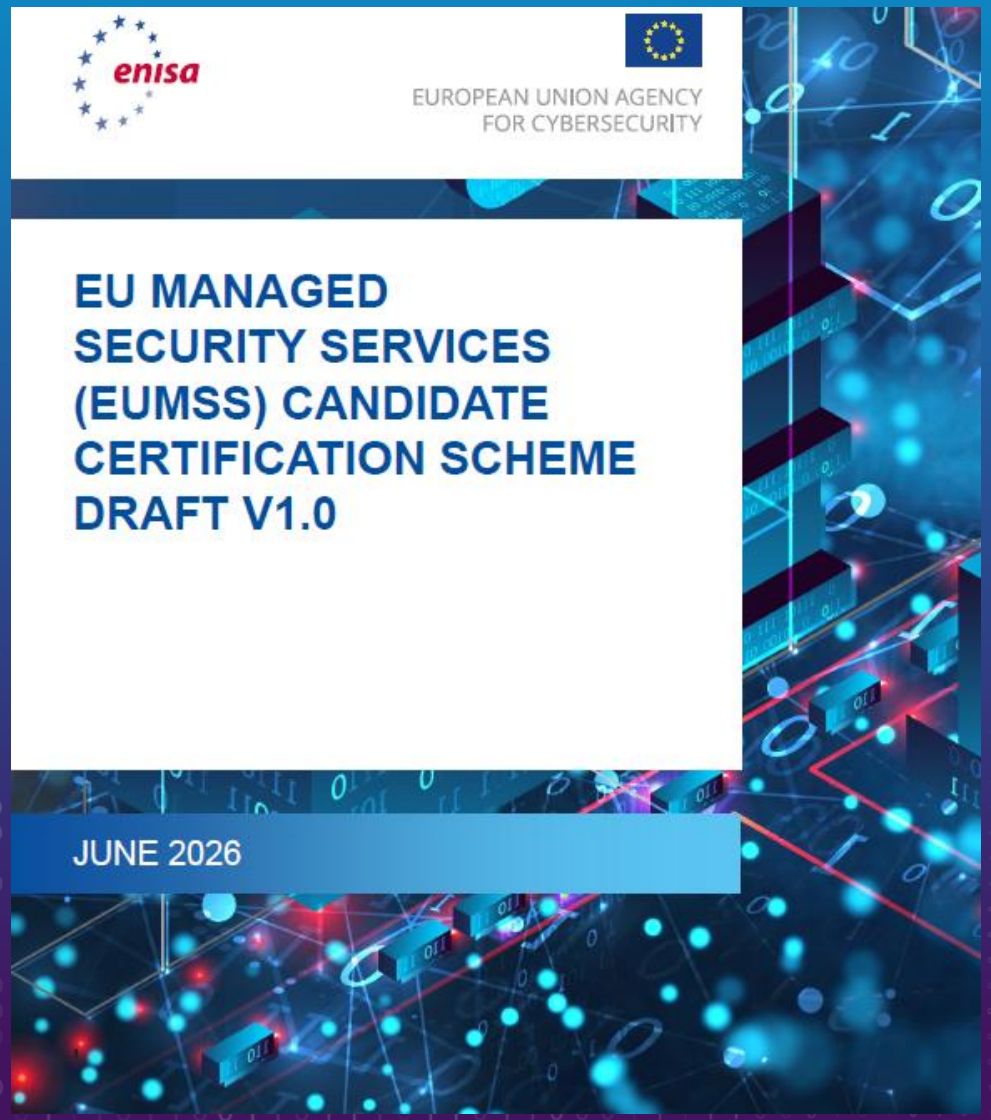
1. NCCA activities “services”

- Cyprus meetings (ECCG, EUMSS, Peer review)
- EUMSS presence and collaboration stakeholders
- Preparation for implementation EUMSS in The Netherlands
  - Identifying and contacting potential CB’s and auditors
  - Aligning supervision (NCCA / NIS2 / DORA)
  - Collaboration Ministry EZK
  - Accreditation
  - Planned – communication website
  - Development policies
- NEN/CEN TS 18072
- Questions / interest: call / info@dutchncca.nl

2. Standards

- NEN CEN TS 18072
  - Scope extension
  - Revision
  - Role EUDIW, EUMSS, EUCS
- NEN CEN TS 18026
  - Potential
  - EUCS
  - Forum Standaardisatie
- Monitoring developments CRA and AIA standards
- Monitoring foundational standards schemes

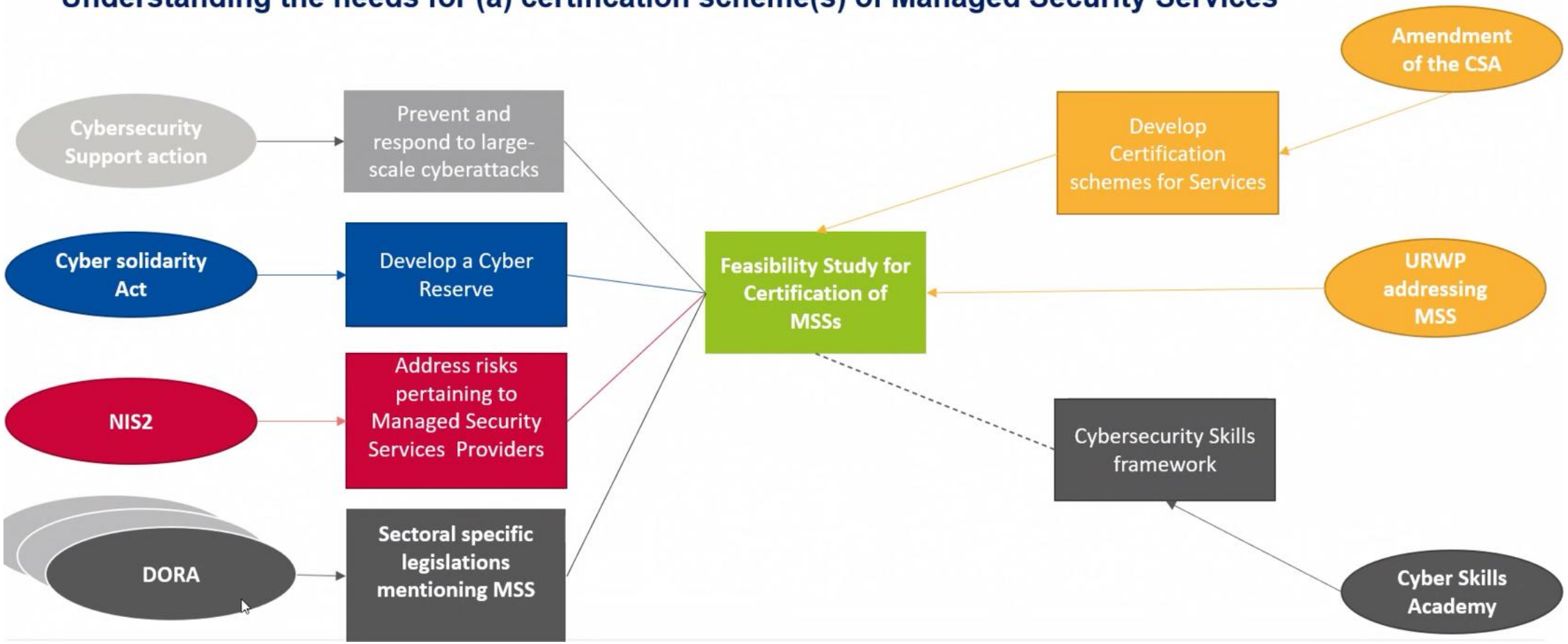
3. EUMSS



- Last Stakeholder meeting explained context
- Delivery version 1
- End July / beginning August Public Consultation
- End September AHWG processing comments
- Final candidate scheme < end of the year
- Legal implementation expected to be worked on in parallel

EU REGULATION BUILDING BLOCKS

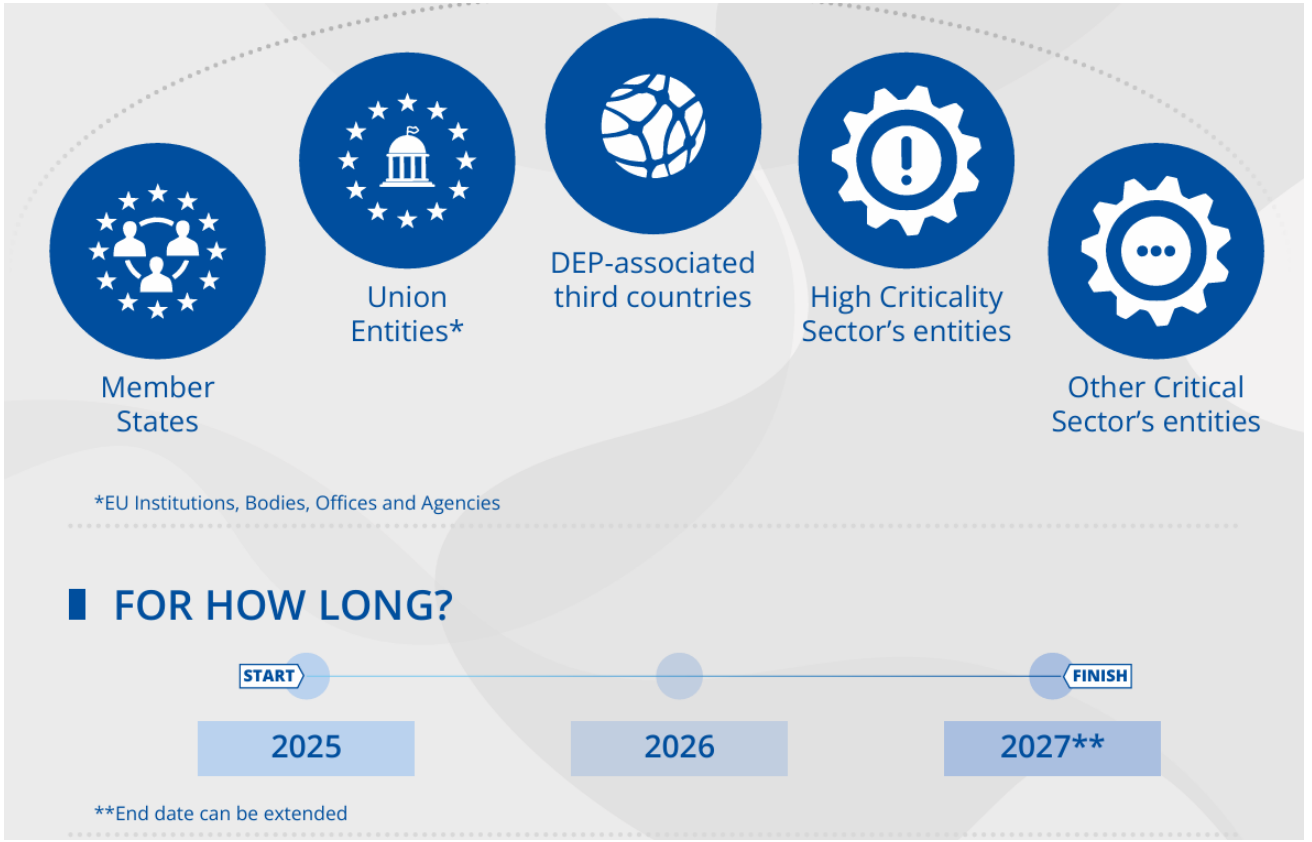
Understanding the needs for (a) certification scheme(s) of Managed Security Services



Picture: previous version D1 Certification of MSS - Contextual Analysis, 2024 ENISA

Cyber reserve

- Deadline of the call for tenders to join the **EU Cybersecurity Reserve** is now extended until 7 July 2026.
- We invite European MSSPs to carefully study requirements per lot and, should they find their companies eligible, apply.
- Please note that, like before, Article 12(5) of the Regulation establishing the Digital Europe Programme applies and this call for tenders is restricted to legal entities established or deemed to be established in Member States and controlled by Member States or by nationals of Member States.



Important!

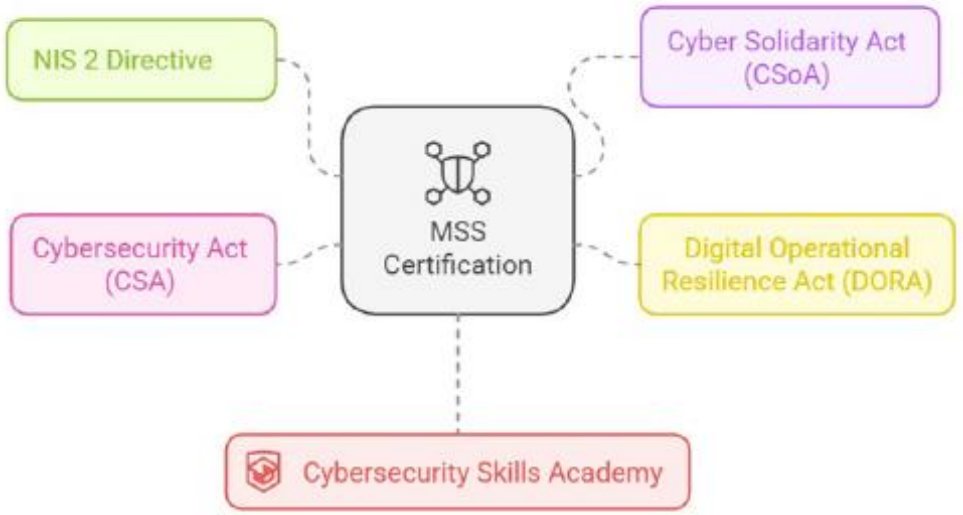


Figure 1. EU legislation and initiatives that could be supported by an EU MSS cybersecurity certification scheme

- CSoA: "Article 17 states that once a European cybersecurity certification scheme for MSS pursuant to the CSA is in place, **the provider shall be certified in accordance with that scheme** within a period of two years after the scheme has entered into application."
- NIS2 article 24: "... may require essential and important entities to use certified solutions"
- Commission Implementing Regulation (EU) 2024/2690 (17 oktober 2024) :" .. recital 17 certification as '**a way to 'obtain assurance** that the ICT products or ICT services to be acquired achieve certain cybersecurity protection levels'

Picture: D1 Certification of MSS - Contextual Analysis_v1.1_en; chapter 3, 2025, ENISA

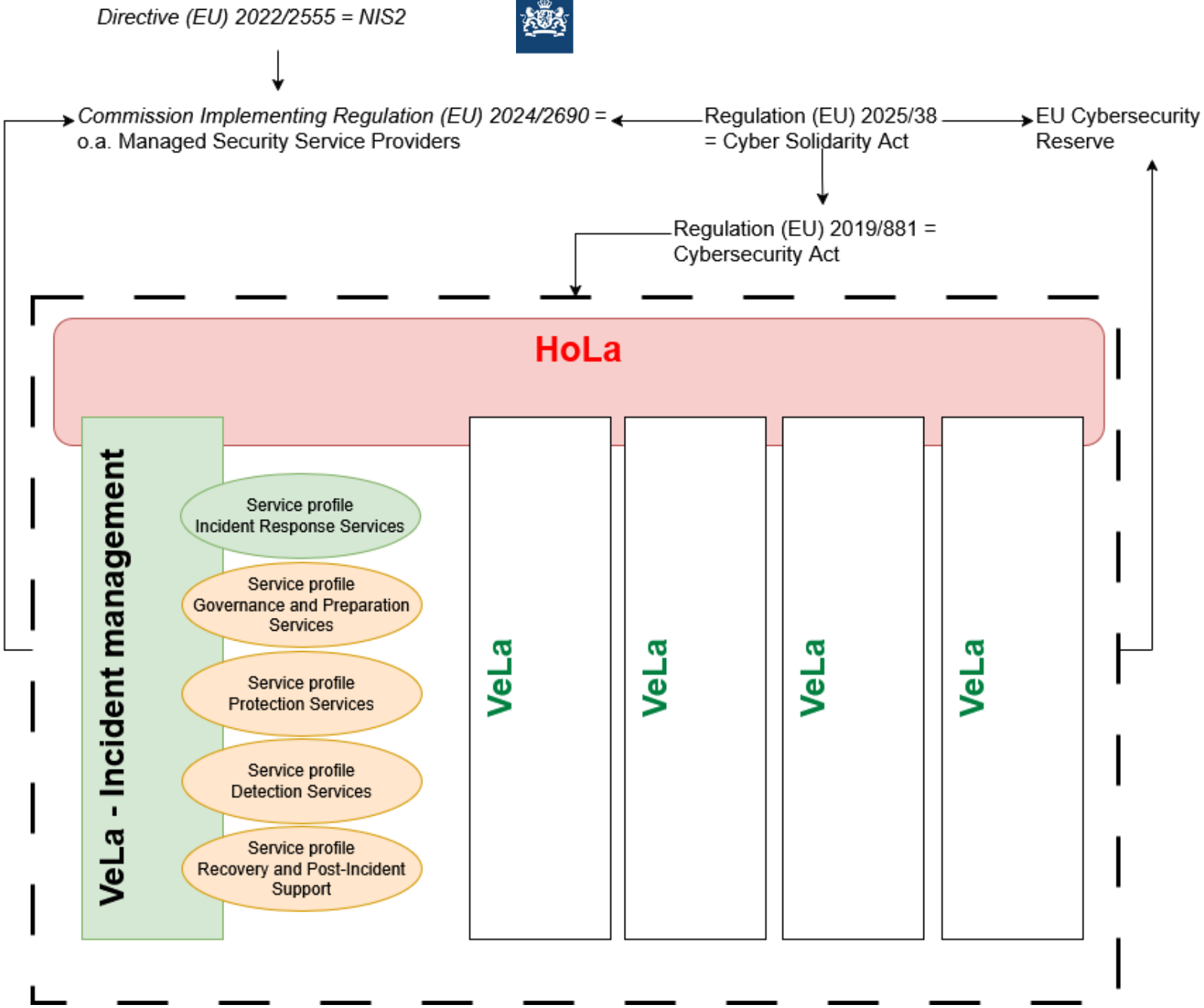
MSS?

- NIS2 definition (art.6): MSSP

  ‘managed security service provider’ means a managed service provider that carries out or provides assistance for activities relating to cybersecurity risk management;

- EUMSS: Service certification # Entity
- EUMSS: future Vertical Layers such as:
  - penetration testing,
  - security audits,
  - consulting related to technical support,
  - cyber threat intelligence provision
  - risk assessment related to technical support.

Version 1 structuring



… and

- Scheme specifications (CAB, Monitoring, non-conformity, protection of information, peer assessment, maintenance, national schemes ceasing, certificate, certification report, certification assessment report, mark and labels)
- HoLa = generic level = ".. provides one common set of baseline cybersecurity, reliability and operational resilience requirements applicable to all Managed Security Services certified under this Scheme. It shall be applied as a mandatory prerequisite for each certified service profile.

  ➔ ?

- VeLa-IM = certification scope
  - General principles
  - Service profiles detailed requirements per Assurance level

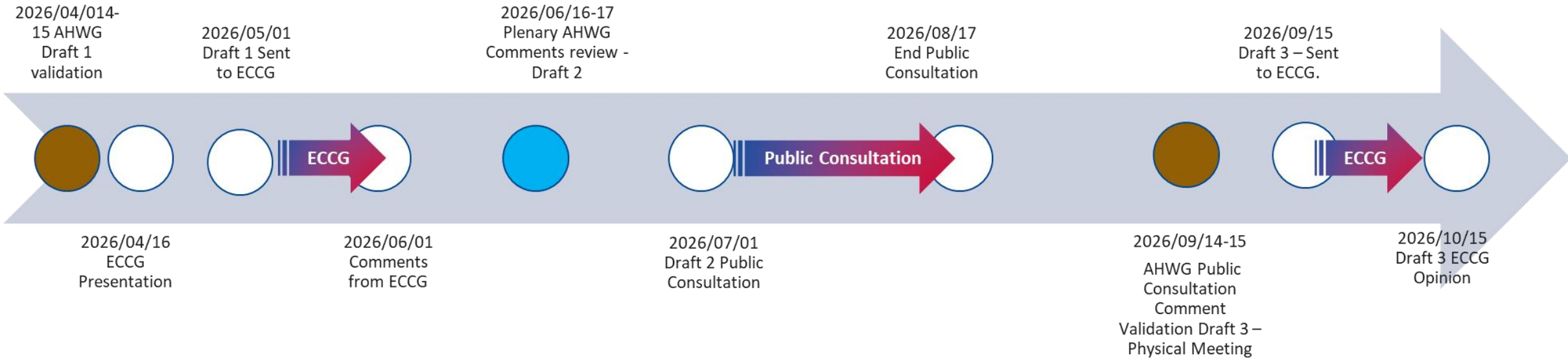
PUBLICATION DATE: JUNE 26, 2025

This report provides technical guidance to support the implementation of the NIS2 Directive for several types of entities in the NIS2 digital infrastructure, ICT service management and digital providers sectors. The cybersecurity requirements for these entities are defined at EU level by Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024. ENISA's guidance offers practical advice, examples of evidence, and mappings of security requirements to help companies implement the regulation.

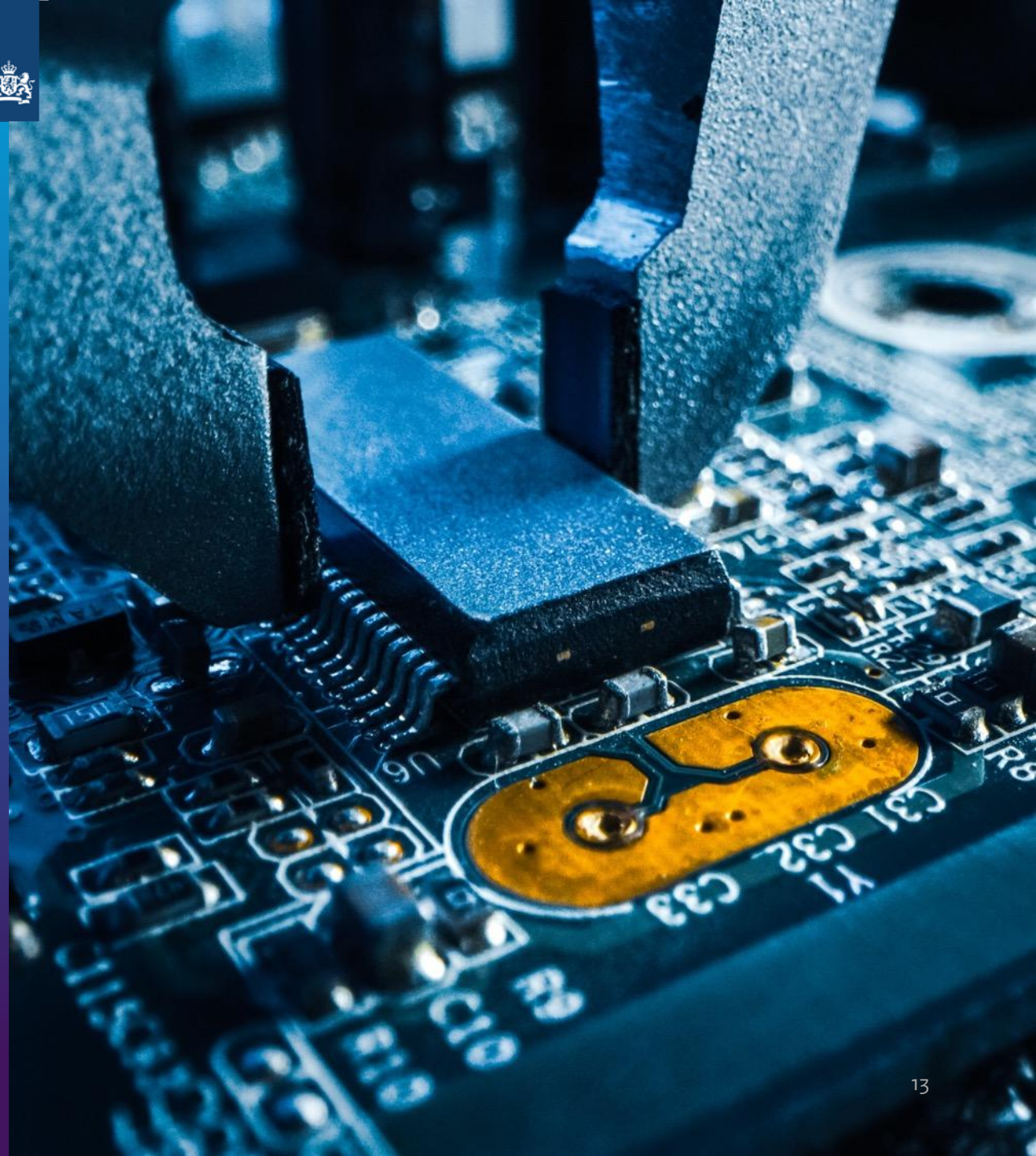
Additional materials

ENISA_Technical_Implementation_Guidance_Mapping_table_version_1.2

Timeline


2026/04/014-15 AHWG Draft 1 validation
2026/05/01 Draft 1 Sent to ECCG
2026/06/16-17 Plenary AHWG Comments review - Draft 2
2026/08/17 End Public Consultation
2026/09/15 Draft 3 – Sent to ECCG.
ECCG
Public Consultation
ECCG
2026/04/16 ECCG Presentation
2026/06/01 Comments from ECCG
2026/07/01 Draft 2 Public Consultation
2026/09/14-15 AHWG Public Consultation Comment Validation Draft 3 – Physical Meeting
2026/10/15 Draft 3 ECCG Opinion

4. CSA 2



What?

- Titel 1: Introduction “Cyber posture”;
- Titel 2: Rol ENISA / EC – larger scope, less influence member states, standards, fees /ECSF
- Titel 3: Corrections CSA 1 and defining Cyber posture / focus technical schemes
- Titel 4: Security of supply chains, Role EC, Role NIS Cooperation Group, sanctions for high risks suppliers, excluding products/services etc

Amendments NIS2

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

- modification Annex I van de NIS2, scope
  - Entity's involved with EUDI Wallet / EU Business wallet
  - Introduction "small mid-cap" → from essential towards important → lighter supervision
- Alignment with "cyber posture" certification to receive "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
  - No involvement in standards / common specifications
  - No CSA certification
  - No accreditation
  - No public procurement participation
  - No EU money

Questions?

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Voor een **veilig verbonden** Nederland

Contact

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

Social Media

#wijzijnRDI