Council of the European Union
General Secretariat

PUBLIC

Brussels, 02 February 2026

WK 1616/2026 INIT

LIMITE

CYBER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	General Secretariat of the Council
To:	Horizontal Working Party on Cyber Issues
Subject:	New Cybersecurity package - Presentation by the Commission

Delegations will find in the annex a presentation given by the Commission at the meeting of the Horizontal Working Party on Cyber Issues on 2 February 2026.

European Commission

PUBLIC

Cyber Security Act 2 (CSA2) **Proposal**

© AdobeStock, Looker_Studio

CNECT 02 February 2026

Overview

PUBLIC

1. Evaluation report
2. Impact assessment
3. Cybersecurity Act 2
4. Directive amending NIS 2 Directive (simplification)

Evaluation Report

PUBLIC



© AdobeStock, Murrstock

Purpose of the report

PUBLIC

Based on **Article 67 of CSA**, an **evaluation** of the **impact and effectiveness** of **ENISA and the ECCF** has been conducted in order **to review ENISA's mandate** and **activities** but also to **assess the ECCF's role** in fostering a secure cyber environment across the EU

Analysis' period:
from 2017 to 2023.

Objective: scrutinise the performance, governance, and working practices of ENISA and the impact, effectiveness and efficiency of the ECCF.

The **evaluation** focuses on **five main criteria**:

1. **Effectiveness**
2. **Efficiency**
3. **Relevance**
4. **Coherence**
5. **EU added value**

Main Findings - ENISA

PUBLIC

1. Effectiveness

ENISA' s mandate fulfilled: **most planned outputs** delivered.

Flexibility demonstrated and positive evaluations from stakeholders, during challenging times such as the COVID-19 pandemic and Russia's war of aggression against Ukraine.

The Agency's size limited its effectiveness, leading to delays and de-prioritisation of important tasks.

Opportunity to enhance effectiveness and efficiency through **improved prioritisation**, **clear focus** and **more strategic resource allocation**.

2. Efficiency

Efficient operations under existing governance structure.

Matrix-based organisational framework helped ENISA's task delivery and foster cooperation between various units.

Stakeholder interaction could be also improved by strenghtening communication channels.
Resource constraints impacted its operational efficiency.

3. Relevance

Ability to review and realign its areas of action to **address emerging developments consistently demonstrated**.

Improve support and increase visibility among diverse sectors and stakeholders, particularly for SMEs, which often struggle to adhere to cybersecurity requirements.

Main Findings - ENISA

PUBLIC

4. Coherence

Strong commitment to fostering cybersecurity cooperation through its **dual approach of direct stakeholder engagement and acting as a facilitator**.

Improve synergies between responsibilities and actions of ENISA **and other EU bodies** such as the European Cybersecurity Competence Centre (ECCC), as well as national cybersecurity authorities. Opportunities for further streamlining and improving operational efficiencies.

5. EU Added Value

Significant contribution to enhancing the EU's cybersecurity ecosystem: facilitated cooperation across the Union, complemented national efforts.

As a decentralised EU Agency, **ENISA's specialised mandate** has allowed it to **consolidate cybersecurity expertise** and **engage effectively with Member States**.

ENISA's current **primary focus on national authorities** has attracted **criticism from private sector stakeholders**. More could be done to tailor insights to the private sector's specific challenges.

Main Findings - ECCF

PUBLIC

1. Effectiveness

Despite challenges, the ECCF **raised awareness** about the importance of cybersecurity certification. The COVID-19 pandemic, while causing operational delays, also underscored the **necessity for resilient digital infrastructure**, thrusting cybersecurity into the policy spotlight.

Inability to effectively address the fragmentation of certification schemes across the EU, mainly due to procedural limitations leading to delays in adoption of schemes. Geopolitical tensions and non-technical debates (e.g. data localisation) further complicated scheme adoptions.

2. Efficiency

Given the lack of implemented schemes, it is **too early to properly assess costs borne or benefits experienced** by stakeholders because of the ECCF implementation. However, survey respondents indicated benefits related to preparatory activities, such as **standards development, capacity building** and **awareness raising**.

Efficiency was hampered due to **several challenges** encompassing both **political and technical dimensions**, which resulted in **significant delays**.

Main Findings - ECCF

PUBLIC

3. Relevance

ECCF's relevance is growing, particularly in **public procurement** of critical infrastructure such as cloud and 5G as well as in enhancing cooperation between EU Member States and streamlining compliance for businesses by providing a single European certification.

Scope and objectives are still relevant in 2024. However, only one scheme exists and only recently became operational, hence there is more potential.

4. Coherence

Synergy with recent cybersecurity legislative developments: some legal acts (e.g. CRA, AI Act) allow for the use of EU certificates as a presumption of conformity with their security requirements, while others include the possibility to make certificates mandatory (e.g. eID, NIS2, CRA).

Required clarifications on interplay on product security between **the CSA and the CRA**.

5. EU Added Value

EU added value compared to what could have been achieved by Member States alone, specifically, in terms of uptake of certification, cost-effective processes, cyber-awareness, trust in the EU single market, and cybersecurity by-default and design, was recognised.

Full potential will only be unlocked once the schemes are fully implemented and maintained.

Conclusions & Recommendations

PUBLIC

ENISA

- **Many positive results in mandate fulfillment, however there is a room for improvement**, especially in the areas of effectiveness and efficiency.
- **Agency's growing list of tasks** raised questions about the possible modification of its mandate. The lessons learned follow two lines:
  1. robust governance structure to ensure effectiveness and **prioritisation**;
  2. **areas** where ENISA's mandate can be strengthened.
- Need to reassess Agency's resources.
- Quality of **stakeholder engagement** is a necessary **determinant** of the Agency's effectiveness, efficiency, relevance, coherence and added value. Therefore, **potential extension of ENISA's tasks** would continue to require active engagement with stakeholders at Member State, EU and industry level.

ECCF

- **Partial achievement of objectives**: improved cooperation and coordination among Member States, EU institutions and the private sector but **delays in the adoption of certification schemes**.
- **Essential EU's role** in bringing together diverse actors to work on shared cybersecurity solutions.
- **Politicisation of debates** (e.g., cloud sovereignty) caused **delays** and reduced stakeholder trust.
- **Positive overall impact** of the intervention with stakeholders recognising the need for coordination on cybesecurity certification.
- Importance of **streamlining reporting requirements**, **improving communication channels** and making ENISA's **outputs more accessible** and **tailored** to stakeholder needs.

Procedural Information

PUBLIC

Organisation and timing

Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework according to Regulation (EU) 2019/881 – STUDY 2023/037, carried out for the European Commission by PwC EU Services EESV, Open Evidence S.L. and PPMI Group, UAB – Final report December 4, 2024.

A Call for evidence on the impact, effectiveness and efficiency of ENISA's mandate and of the provisions of the European Cybersecurity Certification Framework (ECCF) was conducted from 14 July 2023 to 16 September 2023.

The Call for evidence aimed at receiving feedback from relevant stakeholders involved in the cybersecurity domain, and, more specifically, from those involved in the EU certification process.

Overall, 41 stakeholders contributed to the Call for evidence, mostly from the private sector.

Stakeholder Consultation

PUBLIC

Interview Programme

182 individuals were contacted
(40 for ECCF, 142 for ENISA):

- **ENISA: 52 interviews** involving ENISA staff, representatives from DG CNECT, DIGIT, INTPA, NEAR, other EU entities, industry, academia, international Member States' representatives.
- **ECCF: 13 interviews** with 31 interviewees, including EU Institutions, ECCG Members and SCCG Members.

Survey Programme

- An **integrated survey** was conducted to address all stakeholder groups (internal and external).
- The survey included specific sections on ENISA and the ECCF.
- It was conducted **via EUSurvey, 856 stakeholders** received a personal invitation.
- **Results**: **209 responses** were collected, **with 70 respondents (33%) involved with the ECCF**.

Workshops

- **SWOT Workshop**: on 21 May 2024 with 32 participants, including experts from academia, ENISA and the Commission to develop a SWOT analysis for ENISA and the ECCF, validate preliminary findings and foster technical exchange.
- **Recommendations Workshop**: on 12 July 2024 with 77 participants. The workshop presented preliminary evaluation results and facilitated collaborative discussions on lessons learned and potential improvements

Impact Assessment

PUBLIC



© AdobeStock, Shevon

Introduction to the CSA review & problem tree

PUBLIC

The Cybersecurity Act

- Adopted in 2019 to boost cybersecurity, resilience, and trust across the EU.
- Strengthened **ENISA** with a permanent mandate to support policy implementation and coordinate EU-level cybersecurity efforts.
- Launched the **ECCF** to harmonise certification and reduce market fragmentation.

Problem definition *(Why this revision?)*

Misalignment between the Union's cybersecurity policy framework and the stakeholders' needs in an increasingly hostile threat landscape.

Stalled implementation of the ECCF.

Complexity and diversity of the cybersecurity-relevant policies impacting the Union’s cyber posture.

Increasing ICT supply chain security risks.

Directive on Security of Network and Information Systems (NIS2) (2022)

Unified legal framework, cybersecurity requirements for cybersecurity in 18 critical sectors; incident reporting.

Cyber Resilience Act (CRA) (2024)

mandatory cybersecurity requirements for products with digital elements, throughout their whole lifecycle, reporting of vulnerabilities.

EU 5G cybersecurity toolbox (2020)

Recommends measures on how to mitigate risks (technical and non-technical) to 5G networks, incl. restrictions of high-risk suppliers.

PUBLIC

Cybersecurity Act (2019)

Mandate of the EU Cybersecurity Agency ENISA – to contribute to achieving a high common level of cybersecurity across the Union.

Certification – voluntary, to ensure adequate cybersecurity for ICT products, services, processes and managed security services and avoid fragmentation in security assurance.

Cyber Blueprint (2025)

EU framework for Cyber Crisis management.

Cyber Skills Academy (2023)

Communication – coordination of existing training, upskilling and reskilling initiatives for cybersecurity professionals.

Cyber Solidarity Act (2025)

Strengthen capacities.

Funding via European Cybersecurity Competence Centre (2021)

Framework for increasing and coordinated investments in cybersecurity.

GDPR (2016) → CER (2022) → DPRA (2022) → PART-IS (2022-2023) → NCCS (2024) → ...

Overview of policy options - ENISA

ENISA's mandate								
Problem drivers	**Problem**	**Policy option**	**Key measures**	**Specific objectives**				
				SPO1	SPO2	SPO3	SPO4	SPO5
PD1: Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver). **PD2:** Regulatory gaps (horizontal driver). **PD4:** Unsuitable ENISA mandate and resources to evolve with EU cyber ecosystem's and regulatory needs. **PD5:** Complex and fragmented collaboration on cybersecurity among EU agencies, governance bodies and stakeholders.	**P1:** Misalignment between the Union's cybersecurity policy framework and stakeholders' needs in an increasingly hostile threat landscape.	A.1: Clarifying ENISA's mandate and providing for prioritisation.	**M1:** Align with NIS 2, CRA, DORA, CSoA, DORA and NCCS.	☑				
			M2: Ensure for synergies with the ECCC and the Network of NCCs.	☑				
			M3: Prioritise tasks, focusing on policy implementation and sectoral guidelines.		☑			
			M4: Facilitating operational cooperation between Member States and CSIRTs network and EU CyCLONe (cross-border incidents and information flows).	±				
			M5: Adjust budget to reflect additional tasks; limit ad hoc contribution agreements.	±				
		A.2: Reforming of ENISA's mandate.	**M1, M2, M5**	☑				
			M6: Structure the mandate into 3 priority pillars Pillar 1: supporting implementation of general and sector-specific cybersecurity policies and legislation. Pillar 2: providing operational support for MS and enhancing contribution to shared situational awareness and exchange of information. Pillar 3: cybersecurity certification and standardisation.	☑	☑	☑		
			M7: Provide vulnerability management services.	☑	☑			
			M8: Clarify the role and principles of international cooperation.		☑			
			M9: Contribute to the development and maintenance of European individual skills attestations schemes.		☑			
			M10: Resourcing based on EU budget, liaison officers, own resourcing.	☑	☑			
		A.3: Reforming of ENISA's mandate with a strong operational support focus.	**M1, M2, M5, M8, M9**		☑			
			M6, M7, M10	☑	☑			
			M11: Providing direct operational support to NIS 2 entities.	☑	±			
			M12: Create 24/7 operational team with ENISA staff, liaison officers and service providers.	☑	±			

PUBLIC

Overview of policy options - ECCF

European Cybersecurity Certification Framework								
Problem drivers	**Problems**	**Policy option**	**Key measures**	**Specific objectives**				
				SPO1	SPO2	SPO3	SPO4	SPO5
PD1: Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver). **PD2:** Regulatory gaps (horizontal driver). **PD6:** Implementation failure: The practical experience of the development and adoption process of first schemes. **PD7:** Legislative developments not factored in the current ECCF.	**P2:** Stalled implementation of the ECCF.	**B.1:** Clarifying the ECCF's scope, elements and objectives and introducinga maintenance mechanism.	**M1:** Clarifying that ECCF covers technical risk factors only.			☑		
			M2: Formalising maintenance procedure of applicable certification schemes.		☑	☑		
			M3: Aligning the ECCF with the CRA, particularly on vulnerability handling.			☑		
		B.2: Reforming the ECCF by revising its procedures and extending the scope to facilitate simplification of regulatory compliance.	**M1 – M2**		☑	☑		
			M4: Revising procedure for request, development, and adoption of Certification schemes.		☑	☑	☑	
			M5: New Strategic planning and with strengthened stakeholder engagement.			☑		
			M6: Strengthening ENISA's role as 'scheme manager'.			☑		
			M7: Solidifying synergies between the ECCF and CRA / NIS2.		☑	☑	☑	
			M8: Extending scope to cater for future certification of organisation-wide security posture.		☑	☑	☑	
		B.3: Reforming the ECCF as envisaged under option B.2 and introduce mandatory certification for cyber posture.	**M1 – M2; M4 – M8**		☑	☑	☑	
			M9: Empowering the Commission to mandate certification in specific risk-based scenarios and adjust the list.			☑		

PUBLIC

Overview of policy options - Simplification

PUBLIC

Simplification								
Problem drivers	**Problem**	**Policy option**	**Key measures**	**Specific objectives**				
				SPO1	SPO2	SPO3	SPO4	SPO5
PD2: Regulatory gaps (horizontal driver). **PD3:** Vulnerabilities linked to non-technical risks (horizontal driver). **PD8**: Fragmented compliance landscape and complexity of horizontal and sectoral frameworks.	**P3:** Complexity and diversity of the cybersecurity-related policies impacting the Union's cyber posture.	**C.1:** Taking a soft law and non-legislative instruments approach, including the use of existing empowerments (adoption of implementing acts under Article 21(5) and Article 23(11) of the NIS 2 Directive).	**M1:** Harmonise cybersecurity risk-management measures, incident reporting thresholds, as well as information, formats and procedures of notifications to facilitate compliance.				☑	
			M2: Commission to adopt guidelines: • easing the burden on suppliers by clarifying the application of supply chain obligations, • on the scope include NIS 2 definitions to support a more harmonised interpretation, • to streamline ransomware reporting.				☑	
		C.2: Targeted intervention – further simplification of compliance with relevant Union cybersecurity legislative framework.	**M3:** Introduce possibility to demonstrate compliance based on organisational cybersecurity certification schemes in the ECCF.			☑	☑	
			M4: New role for ENISA to support competent authorities in supervision of cross-border entities.		☑		☑	
			M5: Ensure harmonised collection of data on ransomware attacks.	☑			☑	
			M6: Clarifying the scope, definitions and introducing small mid-caps category in NIS2 Directive.		☑		☑	
			M7: Enable maximum harmonisation for NIS2 Directive implementing acts.				☑	
			M8: Guidelines easing the burden on suppliers by clarifying the application of supply chain obligations.		☑		☑	
		C.3: Harmonising cybersecurity-related measures set out in Union legislation.	**M3-M8**	☑	☑		☑	
			M9: Remove all sector-specific risk-management provisions and centralise requirements within NIS 2 Directive ecosystem.				☑	

Overview of policy options – ICT supply chain security

PUBLIC

ICT supply chain security								
Problem drivers	**Problems**	**Policy option**	**Key measures**	**Specific objectives**				
				SPO1	SPO2	SPO3	SPO4	SPO5
PD1: Increasingly hostile and unpredictable threat landscape in a rapidly evolving technological environment (horizontal driver). **PD2:** Regulatory gaps (horizontal driver). **PD3:** Vulnerabilities linked to non-technical risks (horizontal driver). **PD9:** Inadequate measures to address ICT supply chain cybersecurity risks.	**P4:** Increasing ICT supply chains security risks.	**D.1:** Taking a soft law approach to address cybersecurity risks for ICT supply chains.	**M1:** Use of soft law measures within the existing EU regulatory framework to address non-technical risks, with Commission communications, guidance and recommendations.					
			M2: Continuation of coordinated risk assessments under NIS2, with non-binding mitigating measures.					
			M3: Introduction of security requirements on an ad hoc basis in public procurement tenders or auctions.					
		D.2: Ad hoc regulatory intervention codifying the 5G Toolbox.	**M4:** Codification of the 5G Toolbox measures, i.e. mandatory obligation for Member States not to use components from high-risk suppliers in key assets of the network as defined in the EU coordinated risk assessment on 5G security.					±
		D.3: Comprehensive and horizontal framework to address ICT supply chains cybersecurity risks.	**M4**					±
			M5: Horizontal, technology and sector-neutral regulatory framework to address cybersecurity risks, in particular non-technical risks, in ICT supply chains, which would entail: • Identification of key ICT assets and technologies for entities operating in sectors of high criticality and other critical sectors listed in Annex I and II of the NIS2 Directive, through a set of objective and harmonised criteria; • Identification of a list of high-risk suppliers or countries of concern, through a set of objective and harmonised criteria; • Set of proportionate and risk-based measures to mitigate the risks linked to the high-risk suppliers, e.g. storage or processing of data, prohibition to install equipment from high-risk suppliers.			☑		☑

Impacts of the preferred options – Multi-criteria assessment

PUBLIC

The multi-criteria assessment provides a synthetic overview of how each option performs across the main evaluation criteria. The analysis reflects an implicit prioritisation of effectiveness, efficiency and coherence, in line with the nature of the initiative:

Option	Effectiveness	Efficiency	Coherence	Proportionality	Certainty	Overall performance
Low	A.1 B.1 C.1 D.1	B1 B3 (> B1) C1 D1	A.3 C.3	A.3 C.3	A.3 B.3 C.3	
Moderate (Medium)	B.2/B.3 + D.2 A.3 D.2 D.3 + C.1 D.3 + B.1	Al B2 B1 + D3/D2 B3 + D3/D2 C2 D2	A.1 B.1 D.1 D.2	A.1 B.1 B.3 C.1 D.1	A.2 B.2+C.2 D.2 D.3	
High	A.2 B.2/B.3 + D.3 B.2/B.3 + C.2/C.3 C.2/C.3 + A.2/A.3 D.3 D.3 + C.2/C.3	A2 A3 B2 + D2/D3 C3 D3	A.2 B.2/B.3 C.2/C.3 D.3 C.1 C.2 B.2 B.3	B.2 + D.3 B.2 + C.2 D.2 D.3 A.2 B.2 C.2	A.1 B.1 C.1 D.1	**Preferred options** A.2 B.2 + D.3 B.2 + C.2 D.3

Impacts of the preferred options (A2, B2, C2, D3) – Overview

PUBLIC

- Period considered : 2028 – 2032 (five years).
- Quantitative & qualitative assessment ; data limitations related to cyber incidents.
- Key affected stakeholders:
  - Businesses (including SMEs): NIS2 entities; ICT vendors ; Skills attestation providers;
  - Citizens and consumers;
  - Public authorities: NIS supervisory authorities; National certification authorities; ICT users;
  - EU institutions, in particular ENISA.
- Estimated cost savings: EUR 14.6 bn (simplification measures) for businesses & improving EU's overall cyber posture and technological sovereignty.
- Estimated costs: EUR 161.3 M for ENISA; public authorities 80 M; for businesses EUR 3.4 to 4.3 bn per year (for three years) for phasing out 5G equipment from high-risk suppliers

Costs & benefits (2028-2032) – ENISA mandate (A2)

PUBLIC

Economic Benefits

- **Faster Incident Response & detection** reducing cost impacts of incidents (broadly from EUR 3.7 to 4.4 bn over five years).
- Avoided cyber incidents.
- **Skills Attestation**: Expected **lower cost** for individuals, improved **skills portability** and better salary prospects. Development of the cybersecurity skills certification market. Cost avoidance for public authorities.

Costs

- For ENISA – Total: EUR 148.12 M (one-off and recurrent adjustment costs).
- Including:
- EUR 72.6 M (102 FTEs + 40 NLOs).
- Operational costs: EUR 75.5 M (adjustment costs).

Costs & benefits (2028-2032) – ECCF (B2)

PUBLIC

Economic Benefits

- Procedural efficiencies (all actors).
- Market harmonisation (businesses) – certify once, access whole EU market.
- Enhance security levels preventing costs related to cyber incidents (ICT vendors).

Costs (B2+D3) – 6 schemes

- **ENISA** (maintenance): **EUR 13.1 M**
  - EUR 7.9 M (2 FTEs per scheme); EUR 5.2 M (operational).
- **Businesses**: Adjustment and administrative costs:
  - **Cyber posture scheme**: 30 000 administrative recurrent costs (for NIS2 entities: only one-off);
  - **Fees** for maintenance.
- **Public authorities**: **EUR 74,7 M** (FTEs).

Costs & benefits (2028-2032) – Simplification (C2)

PUBLIC

Economic Benefits

- Cost savings for businesses: **EUR 14.6 bn**.
  - Clarifications of scope & removal of micro and small DNS providers: **EUR 13.5 bn** (28 700 entities);
  - Creation of new mid-cap category: **EUR 1.06 bn** (22 500 entities);
  - Cyber posture scheme: **30 M** as of 2032 (1000 certificates issued).
- Cost savings for Public authorities : **EUR 7.5 M**.
- Cost savings due to reduced ransomware attacks.

Economic costs

- Minor adjustment costs for businesses, public authorities, ENISA.

Costs & benefits – ICT supply chain (D3)

PUBLIC

Economic Benefits

- Stimulating new market opportunities for trusted suppliers: **EUR 2bn EUR** per year (recurrent benefits).

Economic costs

- For 5G, **Mobile network operators**:
  - **EUR 3.4 to 4.3 bn** per year (for three years) (one-off cost of replacement of the 5G equipment – adjustment costs).
- For **citizens**, possible (unlikely) transfer costs.
- **Public authorities**: enforcement costs.

Other economic impacts (all options)

PUBLIC

SMEs

- Increased visibility, reputation & harmonisation (vendors, skills attestation providers).
- Market transparency on trusted & secure technologies (ICT users).

Internal market

- Reducing market fragmentation for cybersecurity certification.
- More level playing field for NIS2 entities.
- Harmonisation of ICT supply chain measures facilitating cross-border activities.

Innovation, competitiveness & trade

- Strengthen reputation of European vendors.
- Alleviate regulatory burden.
- ICT supply chain:
  - Boost trusted technology offerings;
  - Availability of alternative suppliers;
  - Engagement with like-minded partners.

Impact on Security and technological sovereignty (all options)

PUBLIC

Impact on security, including hybrid threats

- Overall level of security in the Union pushed upwards.
- Reduction of the exposure to hybrid attacks or cybersecurity incidents by developing expertise and enriching vulnerability records.
- Capacity development to better address in particular hybrid threats, enhanced cooperation with other specialised agencies.
- Development of a skilled cybersecurity workforce.

Impacts on technological sovereignty, open strategic autonomy, security of supply

- Decrease of the dependency on high-risk suppliers or entities originating from or controlled by countries posing cybersecurity concerns at Union level.
- Fostering a European industrial cybersecurity ecosystem, including through a greater involvement on standardisation.
- Fostering user trust and reputation of European players.

Mandate of ENISA

PUBLIC



© AdobeStock, Thanadon88

Revision of the mandate of ENISA

PUBLIC

Why?

- Need to meet stakeholders' needs in an increasingly hostile threat landscape.

What?

- Revise ENISA's mandate accordingly.
- Streamline it into 4 "Pillars".

How?

- By aligning its governance structure to the tasks that have been added by recent initiatives (ie. Cyber Resilience Act; Cyber Solidarity Act).
- By improving the existing tasks.
- By identifying areas with a need to strengthen ENISA's mandate.

ENISA's mandate in short

Area	CSA	CSA2 proposal
EU policy support	Guidelines, reports, through NIS Cooperation Group Capacity-building Research and innovation tasks International cooperation	Clear emphasis on support in implementing cybersecurity laws and policies Tailored support to specific sectors (i.e. health) Capacity-building International cooperation in line with EU policies/priorities
Standards and certification	ENISA monitoring standards for schemes only	ENISA drafting technical specifications to support Union legislation, e.g., CRA and certification ENISA actively contributing CRA standardisation and international standards
Operational cooperation	ENISA secretariat of EU-CyCLONe and CSIRTs network	ENISA member of CSIRTs network Situational awareness (sharing early warnings, analysis, use of secure communications tool) Stronger role in vulnerability management (e.g., enriching vulnerability services, providing advisories) Managing platforms for incident and vulnerability reporting Support for incident response
Skills	No concrete tasks – objective only	Implementation of Cybersecurity Skills Academy Develop European cybersecurity skills attestation schemes and authorise providers to deliver attestations
Ransomware	-	Helpdesk to help entities respond to and recover from ransomware attacks, in cooperation with Europol Monitor trends in techniques, demands and impact of ransomware attacks

PUBLIC

ENISA's mandate

Section 1 – Support for implementation of Union policy and law

PUBLIC

Support for implementation

- Technical guidance for supporting consistent implementation of EU cybersecurity acquis
- Leverages ENISA's expertise where it can provide added-value

Assistance in diverse range of capacity-building activities

- Example: ENISA to share information with the ECCC about current and emerging risks and cyber threats (ensures synergies between the ECCC and ENISA)

ENISA's mandate

PUBLIC

Section 1 – Support for implementation of Union policy and law (cont.)

Awareness-raising and talent pool

- Task focused on promoting visibility of Union policies and laws by developing actionable tools and guidance
- Adding support initiatives aimed at increasing European cybersecurity talent pool (e.g., cybersecurity competitions)

Market knowledge and analyses

- Disseminate analyses of main market trends in the cybersecurity market

International cooperation

- Cooperation carried out in line with the Union priorities

ENISA's mandate

Section 2 – Operational cooperation

PUBLIC

Reinforced operational cooperation to match the needs

Focus on improving shared situational awareness

ENISA's role strengthened – ENISA becomes a member of the CSIRTs network

A number of new tasks (see next slides)

ENISA's mandate

Section 2 – Operational cooperation (cont.)

PUBLIC

Early alerts to CSIRTs / EU-CyCLONe

- In case of potential/ongoing significant or large-scale incident, or
- cyber threat of a potential cross-border nature

Early alert service offered to NIS2 entities

- About cyber threat indicators and recommended mitigation measures

Ransomware

- Monitor trends in techniques, demands and impact of ransomware attacks
- Provide such information to the CSIRTs network, EU-CyCLONe, the Commission and Europol
- Support incident response: create a **helpdesk** to help NIS2 entities in responding and recovering from a ransomware incident

ENISA's mandate

Section 2 – Operational cooperation (cont.)

PUBLIC

Vulnerability management

- Develop a common Union vulnerability management service capacity
- Provide targeted vulnerability management services to stakeholders, related to the European vulnerability database

Provision of tools and platforms

- General mandate to provide and operate tools and platforms provided by law
- Examples: single reporting platform under CRA; single-entry point for incident reporting under amended NIS2

ENISA's mandate

PUBLIC

Section 3 – Cybersecurity certification and standardisation

Cybersecurity certification

- Updated provisions to reflect the new framework
- Clear list of activities that ENISA carries out with respect to certification schemes
- **Novelty** – ENISA in charge of maintaining schemes
- Clear list of activities for which ENISA provides support to the Commission in the context of the ECCF

Standardisation

- Draft technical specifications and guidance to support implementation of Union cybersecurity law, considering European and international standards

Cryptographic algorithms

- Support the development and evaluation of cryptographic algorithms
- Where a cryptographic algorithm evaluated positively, ENISA to cooperate with EU standardisation bodies to support its standardisation

ENISA's mandate

Section 4 – Implementation of the Cybersecurity Skills Academy

PUBLIC

Objectives

- Supplement MSs actions in addressing shortage of cybersecurity professionals:
- Ensure skills portability across MSs
- Support the emergence of new providers

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

- Provides a common understanding of relevant cybersecurity roles and associated tasks, skills and knowledge

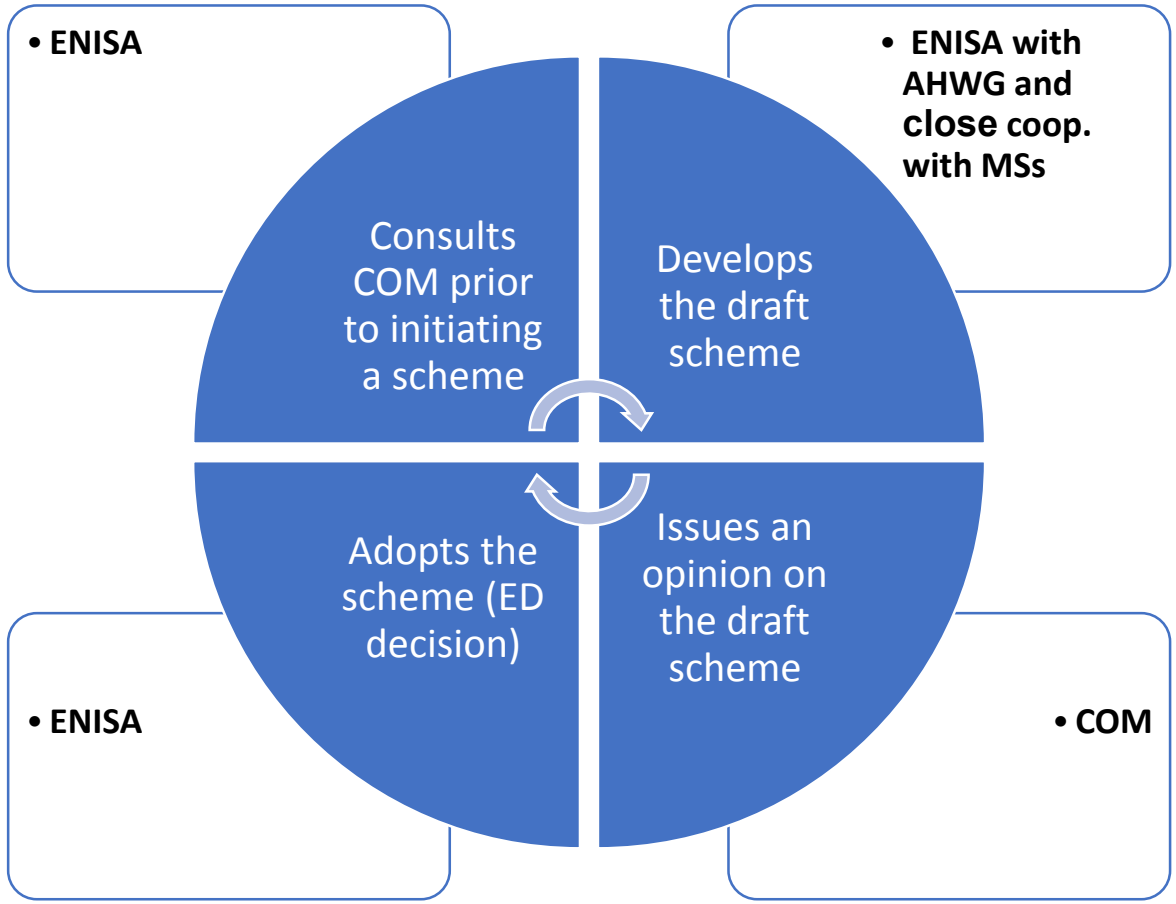
European individual cybersecurity skills attestation schemes

Background: pilot projects on an attestation scheme (ENISA-led, 8 MSs)

Definition: "a comprehensive set of rules, requirements, standards and procedures established by ENISA and associated to a role profile of the ECSF or a subset thereof, and that apply to and are applied by authorised attestation providers"

Voluntary uptake

European cybersecurity skills attestation schemes: development, maintenance and adoption



In practice: issuance of attestations

Individual applies to an authorised attestation provider

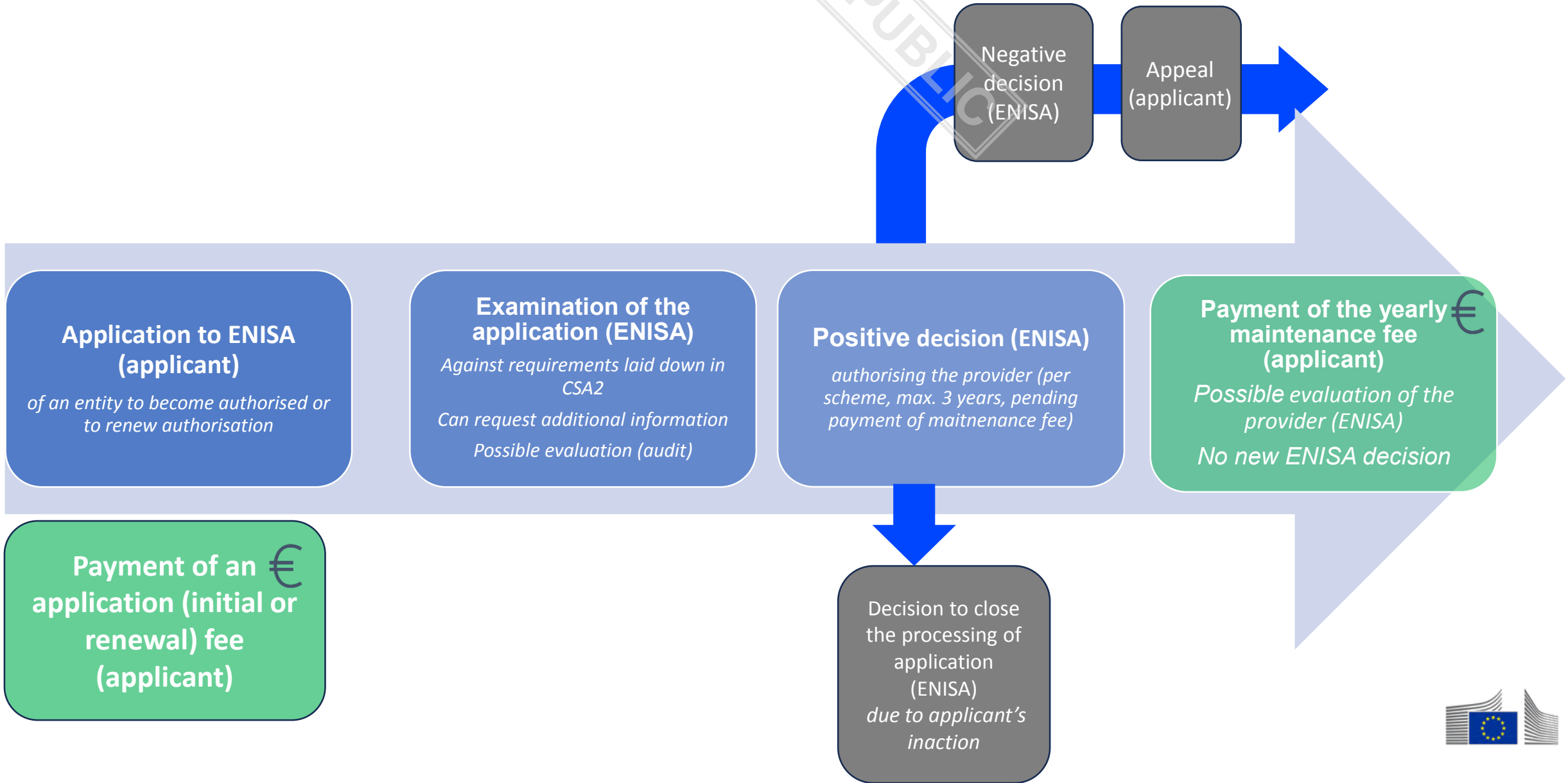
Authorised attestation provider assesses the candidate against the scheme (provider may charge a fee)

Positive assessment = Provider issues the attestation

PUBLIC

Authorisation of providers (overview)

PUBLIC



Fees

PUBLIC

What

Fees for:

- issuing authorisations (examination of application evaluation)
- yearly maintenance of the authorisation;
- renewing authorisations (examination of application, evaluation)

How

Implementing acts to:

- determine the fees to be levied by ENISA,
- the ways and conditions under which the fees should be levied

ENISA's mandate

Section 5 - Structure and organisational aspects

PUBLIC

Management Board of ENISA

- Need to enable strategic discussions to provide strategic directions to ENISA
- Composed of heads of a national competent authority designated under NIS2 (+ Commission, as today)
- If not feasible, another high-level representative

No Network of Liaison Officers (replaced by liaison officers delegated on a permanent basis to ENISA)

Member States to designate 2 Liaison Officers

- To reinforce operational cooperation effectively

European Cybersecurity Certification Framework

PUBLIC



© AdobeStock, loechai

New European Cybersecurity Certification Framework

PUBLIC

What? Eligibility?

- Cybersecurity certification increases **trust and security** in the internal market.
- Voluntary, companies can get confirmed by an independent authority security from cyber threats against recognized security standards.
- A certificate indicates the **level of cybersecurity** of a product or service and hence increases **transparency** in the internal market for users.
- Certification ICT product, services, processes and managed security services or **cyber posture**
- **Technical risk factors**
- **High-risk suppliers and their key ICT assets** excluded from certification

Certification as Compliance Tool

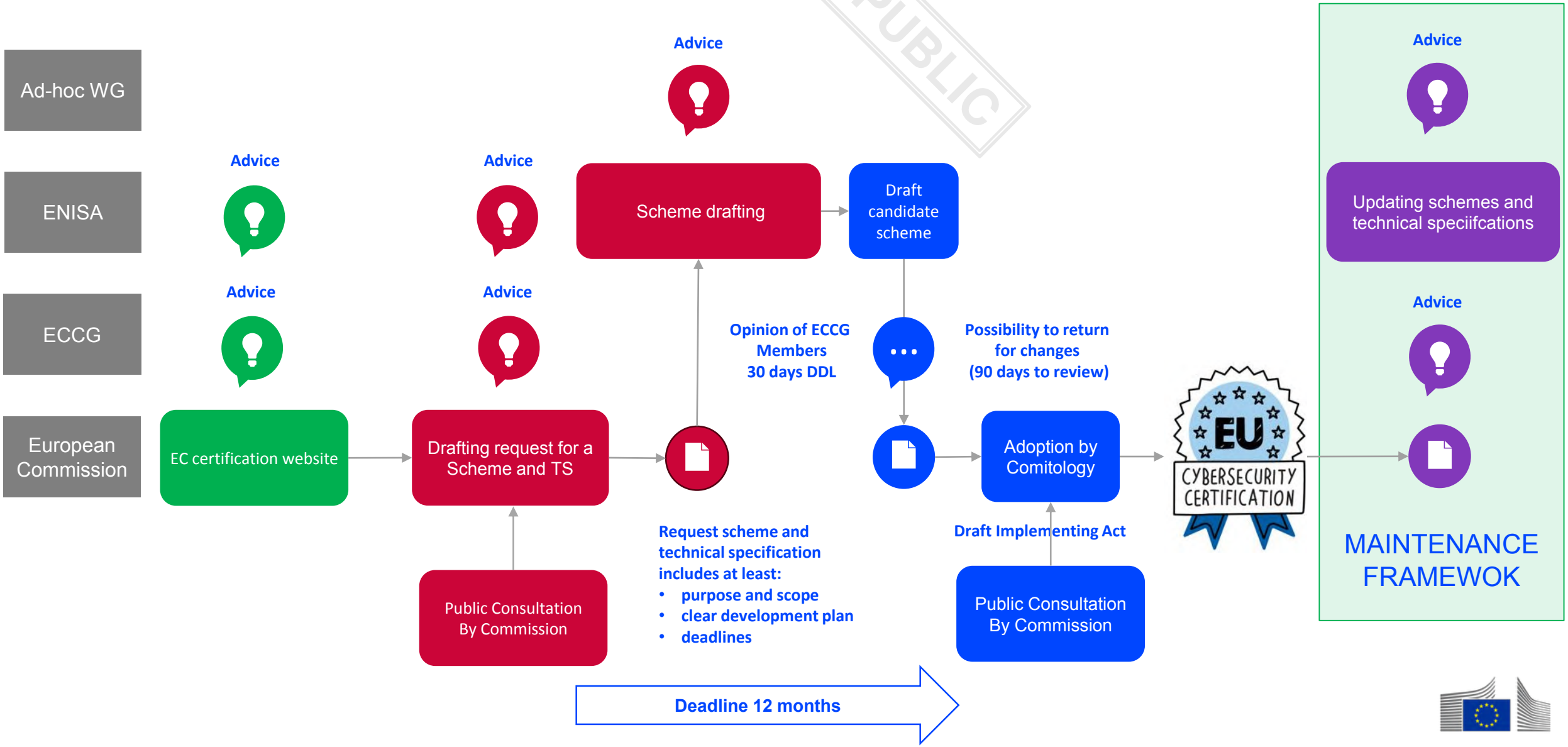
PUBLIC

Certification

- updated and **fully synergised** with existing Union law
  (alignment with the CRA on security objectives, notification of CABs and supplementary information)
- as a **simplification tool** to demonstrate compliance with CRA & NIS2 and potentially other legal acts
  (organisation cyber posture scheme to enable complified compliance)
- harmonised across schemes through **model provisions**
  (user-friendly reference provisions to harmonise templates across schemes)

Streamlined procedure promoting accountability

PUBLIC



ECCF: Who does what?

PUBLIC

Member States

The scheme "*owner* "	The scheme "*manager*"	Advisor & operational enforcer
• Oversight of the procedure and implementation • Strategic planning and requesting of schemes • Adoption and review of schemes	• Scheme development and maintenance • Support of policy implementation • Developing certification ecosystem	• Consulted in every step of the way (ECCG, Comitology) • Certification issuers through NCCAs • Accreditations and authorisations

Fees

PUBLIC

What

Fees for:

- For issuing European cybersecurity certificates (certificate holders)
- For conformity assessment bodies activities

How

Implementing acts to:

- determine the fees to be levied by ENISA,
- the ways and conditions under which the fees should be levied

Enhanced transparency and stakeholder engagement

PUBLIC

Regulation 2019/881:

- **ENISA certification website**
- **Comitology**
- **Stakeholder input in scheme development**
- ~~Union Rolling Work Programme~~
- ~~Stakeholder cybersecurity certification group~~

The new CSA2:

- ENISA certification website
- Comitology
- Stakeholder input in scheme development **+**
- **European Cybersecurity Certification Assembly** (new)
- **COM certification website** (new)
- More public consultations