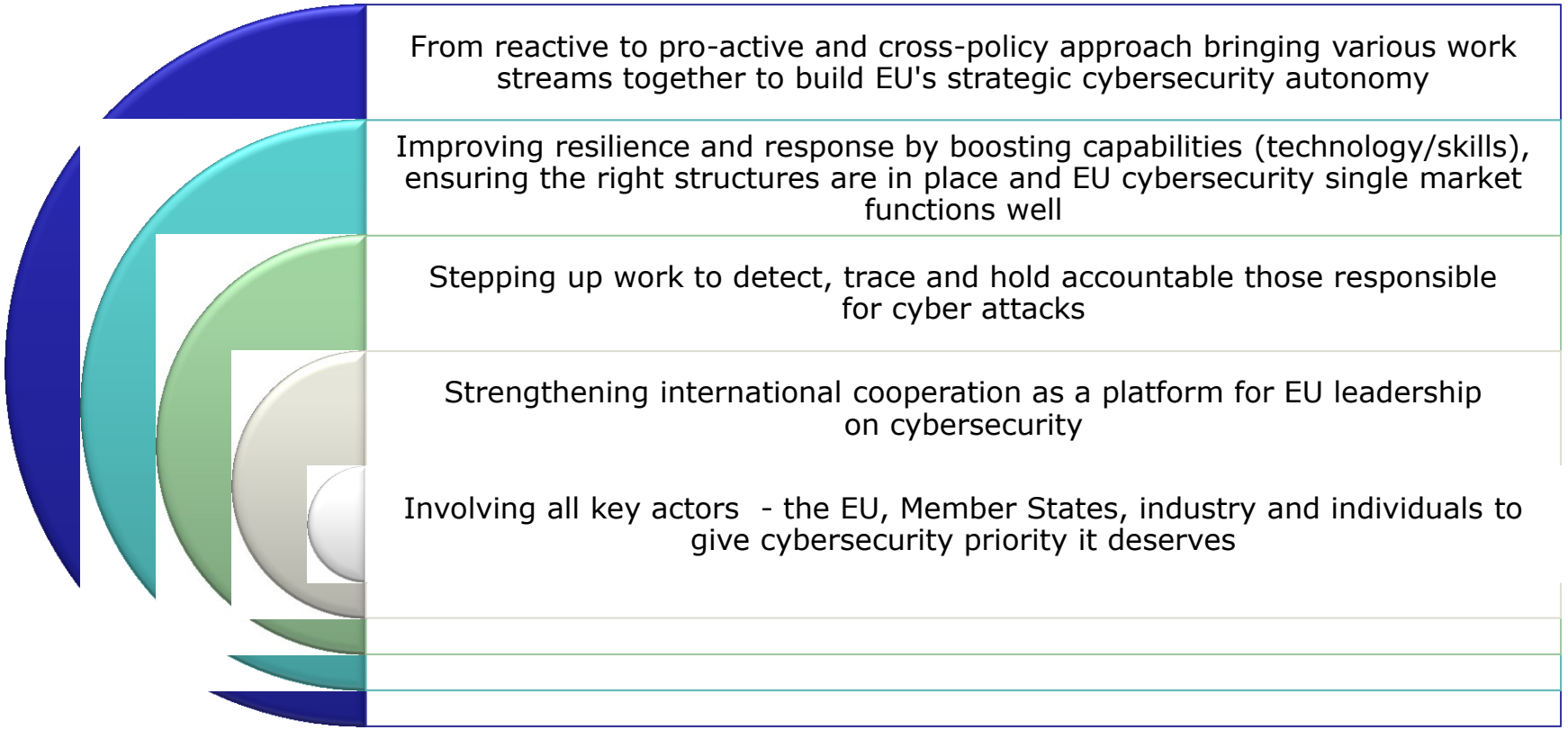
Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

Building strong cybersecurity for the EU: Resilience, Deterrence and Defence



	Building EU Resilience to cyber attacks	Creating effective EU cyber deterrence	Strengthening international cooperation on cybersecurity
Cybersecurity Act	Reformed ENISA	Identifying malicious actors	Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
	EU cybersecurity Certification Framework	Stepping up the law enforcement response	Strengthening cyber dialogues
Communication	NIS Directive Implementation	Stepping up public-private cooperation against cybercrime	Modernising export controls, including for critical cyber-surveillance technologies
Recommendation	Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund	Stepping up political response	Continue rights-based capacity building model
	Cybersecurity competence network with a European Cybersecurity Research and Competence Centre	Building cybersecurity deterrence through the Member States' defence capability	Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence
	Building strong EU cyber skills base, improving cyber hygiene and awareness		

ICT cybersecurity certification

Towards a true cybersecurity single market in the EU

The issue

*The **digitalisation** of our society generates greater need for **cyber secure** products and services*

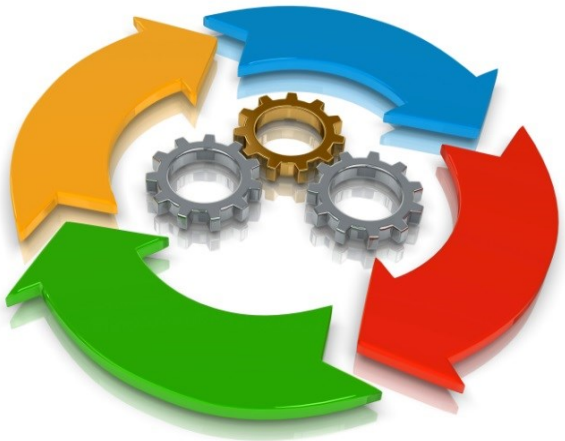
*Cybersecurity **certification** plays an important role in increasing trust of digital products and services*

Current landscape

- *emergence of separate national initiatives lacking mutual recognition (e.g. France, UK, Germany, Netherlands, Italy)*
- *Current European mechanisms (SOG-IS MRA) have limited membership (12 MSs), involve high costs and long duration*

Our proposal

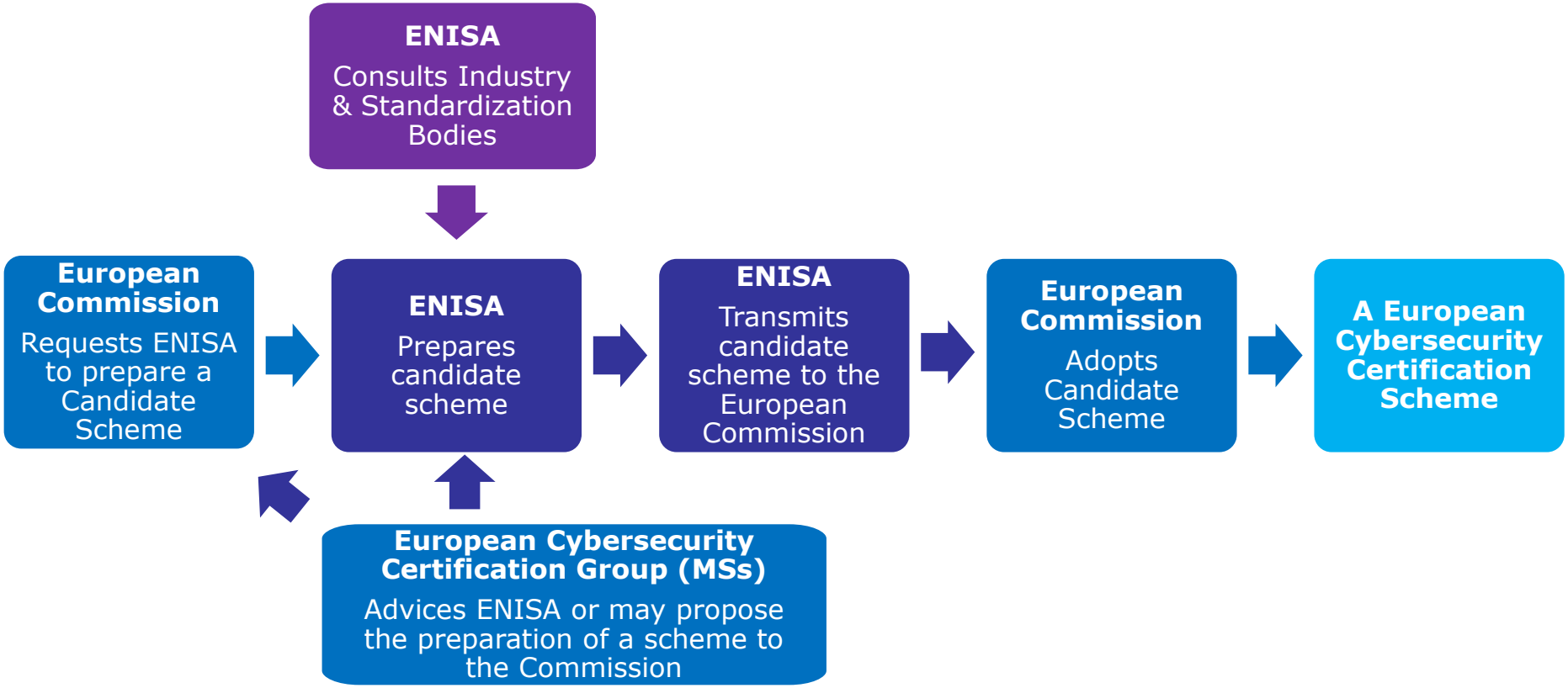
*A **voluntary European** cybersecurity certification **framework….***



*…to enable the creation of individual EU certification **schemes** for ICT products and services…*

*…that are **valid across the EU***

How will the framework work in practice



In a nutshell: EC proposes & decides, Group advices (and may propose), ENISA prepares schemes

Core elements (i)

- ***No 'One size fits all' - one EU Framework, many schemes***
- *Each scheme will specify:*
  - i) scope (pdct/service), ii) evaluation criteria, iii) assurance level, iv) security requirements v) rules for monitoring compliance
- *Certificates from European schemes are valid across **all MSs**.*
- *Where a **European scheme exists**:*
  - MSs cannot introduce new national schemes with same scope
  - Existing national schemes covering same pdct/service cease to produce effects
  - Existing certificates from national schemes are valid until expire date
- *The use of EU certificates remains **voluntary**, unless otherwise specified in Union law.*
- *A EU scheme **should not conflict** with certification provisions from **other Union legislation** (e.g. data protection certification in GDPR).*

Core elements (ii)

National Authorities and European Cybersecurity Certification Group (ECCG)

***MSs** will appoint a **national certification supervisory authority**. In their territory, each authority shall:*

- ***supervise** the activities of conformity assessment bodies (**CAB**) and the compliance of the certificates issued by CABs*
- *be independent of the entities they supervise.*
- ***handle complaints** on certificates issued by CABs*
- ***withdraw certificates** that are not compliant and impose **penalties***
- ***participate** in the new European Cybersecurity Certification Group*

*The **Group** has the following tasks:*

- ***advises** the Commission and assists ENISA in the preparation of EU schemes*
- ***proposes** to the Commission that it requests ENISA to prepare a EU scheme*
- ***adopt opinions** addressed to the Commission relating to the maintenance and review of existing EU schemes*
- *The Commission chairs the Group and provides the secretariat with the assistance of ENISA*

Core elements (iii)

National Accreditation Bodies (NABs) & Conformity Assessment Bodies (CABs)

- *European cybersecurity **certificates** are normally **issued** by **CABs accredited** by a National Accreditation Body (**NAB**) – Reg. 765/2008*

  - Accreditation shall be issued for a maximum of five years

  - NABs can revoke accreditation of CABs

  - NABs notify the Commission of the accredited CABs for each EU scheme

- ***However**, in **justified cases** a European scheme may provide that a **certificates** can only be **issued by a public body** such as:*

  - *a national certification supervisory authority*
  - *a body accredited as a CAB*
  - *a body established under national laws, meeting the requirements according to ISO/IEC 17065:2012.*

Benefits…for citizens/end users

NOW

Difficult to distinguish between more and less secure products/services

Co-existence of schemes makes comparison difficult…

…end-users (OES) refrain from buying certified products/services

FUTURE

more information on the security properties of product/services ahead of purchase

Greater incentive for OES to buy certified products/service

Increased cyber resilience of critical infrastructures

*…As end-users of digital solutions, **governments** would rely on an institutional framework to identify and express priority areas needing ICT security certification.*

…For vendors/providers

The possibility to obtain cybersecurity certificates that are valid across the EU would:

- *Generate higher incentive to certify and enhance the **quality** of digital products / services*
- *Enhance **competitiveness** through reduced **time** and **cost of certification***
- *Help gain access to market segments where certification is required*
- *Contribute to promote a **chain** **of** **trust** **between** vendors* **and** *end-users*

*For **SMEs** and **new business…***

- *Elimination of a potential market-entry barrier*

European Commission

Thank you for your attention!