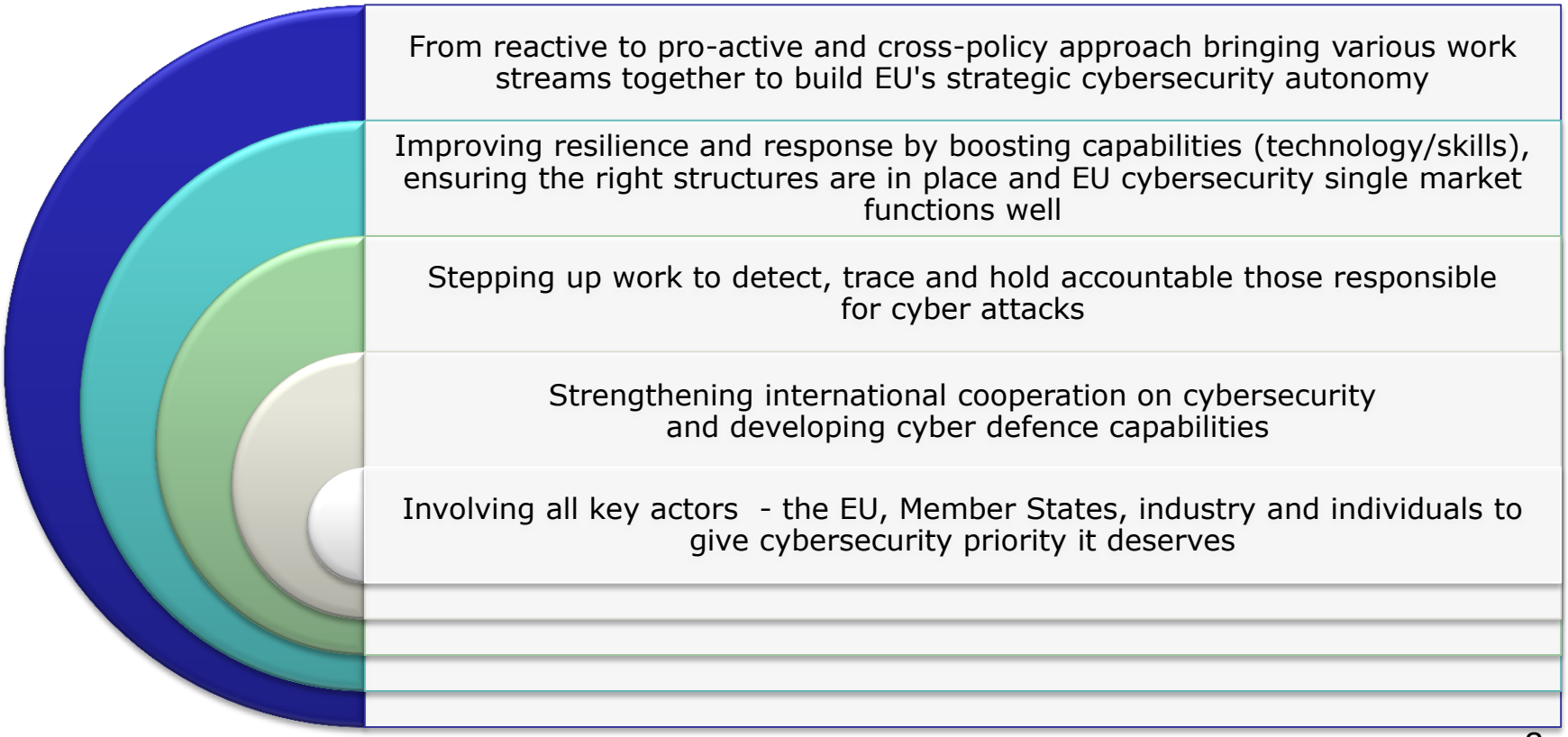
# Resilience, Deterrence and Defence: Building strong cybersecurity for the EU

# 2013-2017: Evolving threat landscape

- Proliferation of (poorly secured) IoT devices
- Blurring lines between state and non-state actors
- Hybrid attacks on western democracies
- Fake news
- Evolving cybercrime business models
- Cyber espionage on the rise
- Dependence on foreign security technologies
- Persisting critical infrastructure vulnerabilities
- Attempts to promote new internet governance model
- Vulnerabilities of third countries

# 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 | Advancing EU 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 and diplomatic 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 capabilities | Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence |
| | Building strong EU cyber skills base, improving cyber hygiene and awareness | | |

# Cybersecurity Package

## *Highlights of key initiatives*

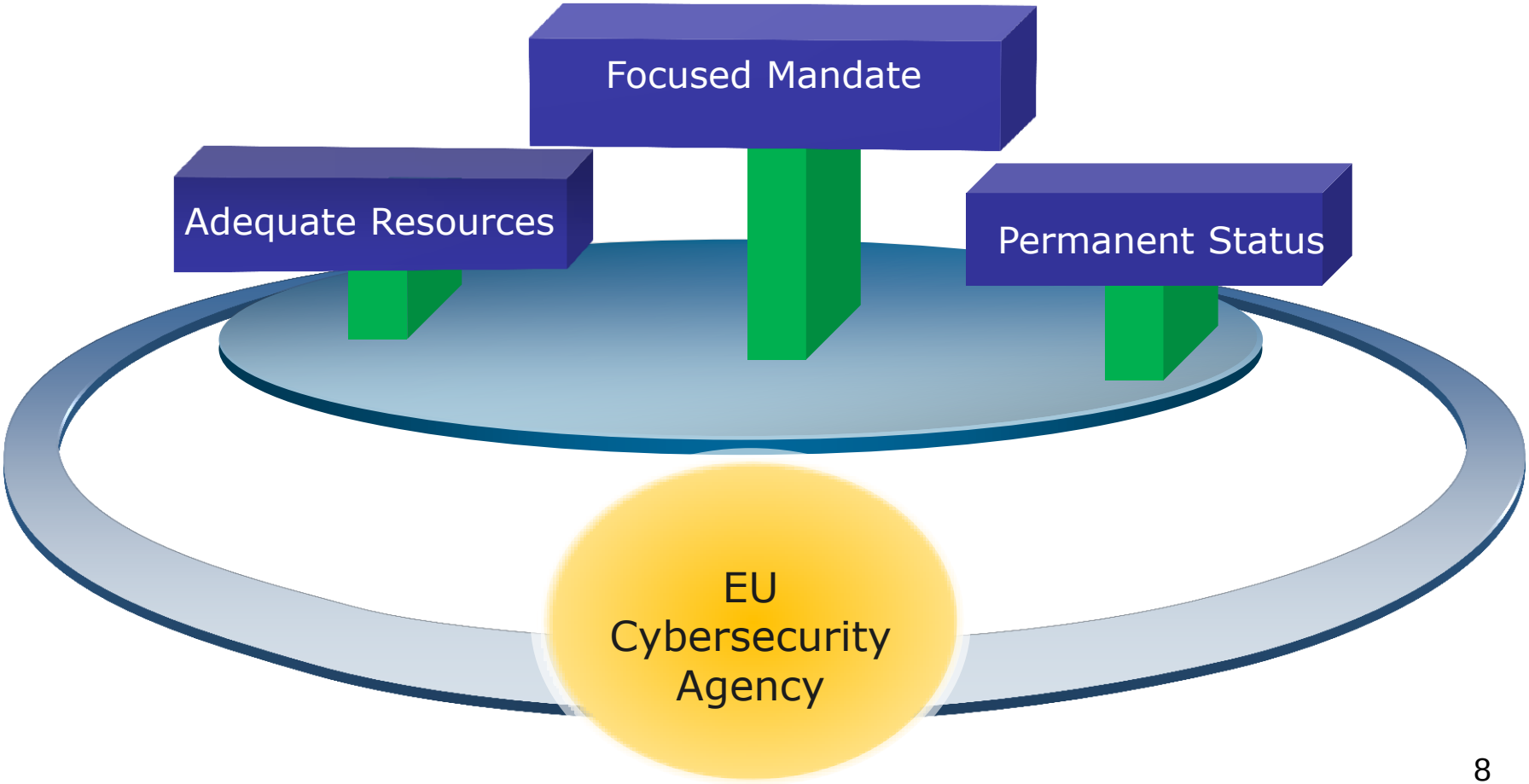
# EU Cybersecurity Act

**Towards a reformed**
**EU Cybersecurity Agency**
**and reinforcing the cybersecurity single market in the EU**

# ENISA

## Towards an EU Cybersecurity Agency fit for current and future challenges

# What's new with the new proposal?



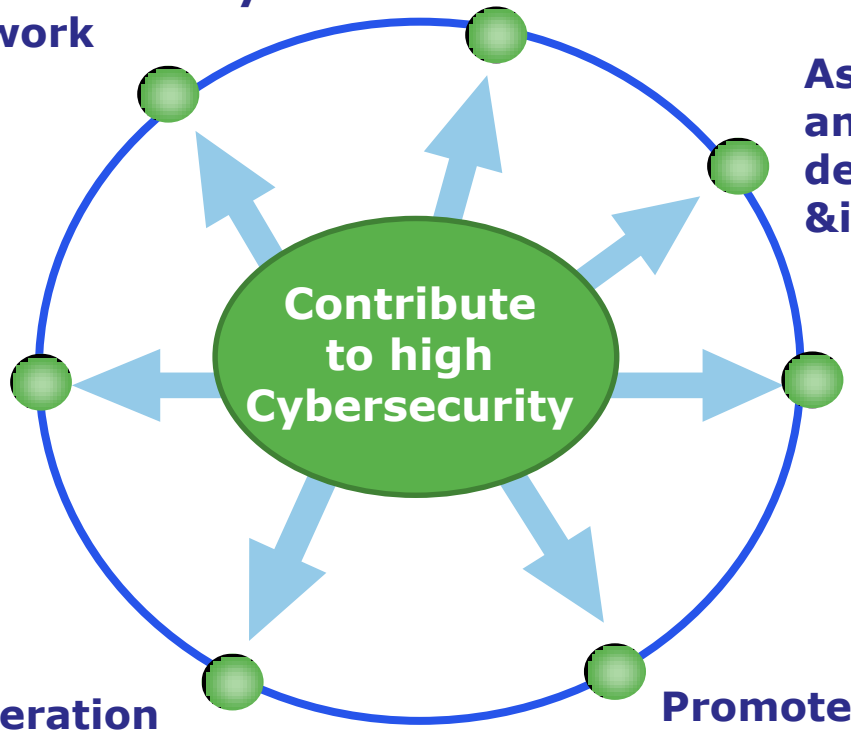
# Mandate and objectives

**Promote the use of certification & contribute to the cybersecurity certification framework**

**Be an independent centre of expertise**

**Assist EU Institutions and MSs in policy development &implementation**

**Increase cybersecurity capabilities at Union level to complement MSs action**




**Support capacity building & preparedness**

**Promote cooperation &coordination at Union level**

**Promote high level of awareness of citizens & businesses**

# Policy&Law

## Development

- horizontal cybersecurity policy&law
- sectoral policy with cyber angle
- electronic identity and trust services
- security of electronic communications

## Implementation

- NIS Directive
- other Union cyber policy&law
- electronic identity and trust services
- security of electronic communications

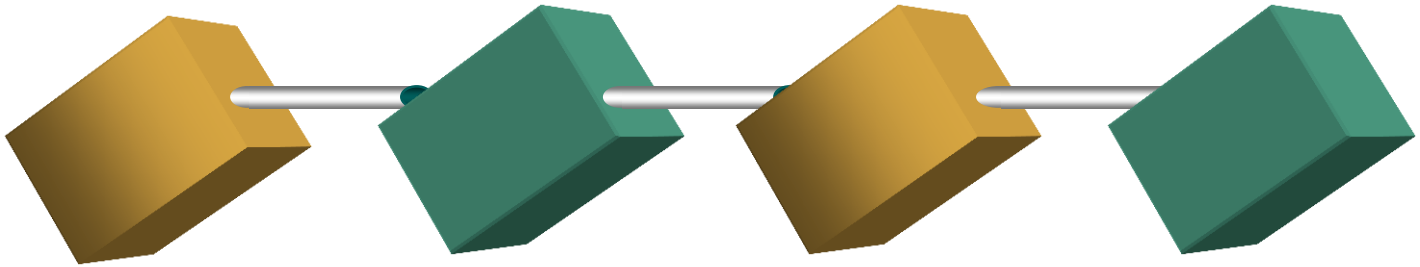
## Review

- Annual report on the state of implementation of legal framework

**ENISA**

Advises & Contributes

# Capacity building



CSIRTs Development, national Strategies, support to Cooperation Group

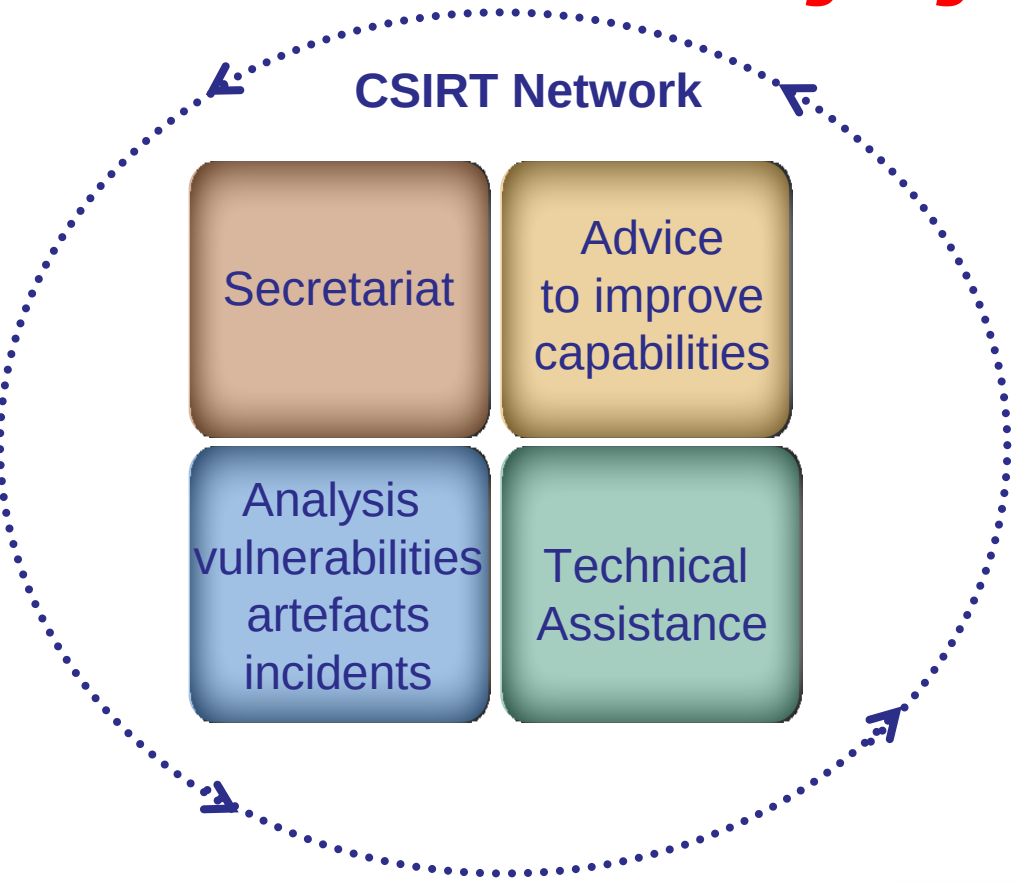
Facilitate Establishment & development Sectoral ISACs

Trainings, Knowledge, Expertise

Support development & Review of Union strategies

# Operational cooperation (1/2)

***Ongoing cooperation***





Regular *EU Cybersecurity Technical Situation Report*


*Annual cybersecurity exercise*

# Operational cooperation (2/2)

*Significant Incidents&Crises*

- Provide support to or carry out an ex-post technical enquiry
- Contribute to develop a cooperative response to large-scale cross-border incidents or crises (Blueprint):
  a) aggregating reports from national sources to contribute to common situational awareness;
  b) ensuring the efficient information flow and escalation mechanisms between the CSIRTs Network and the technical and political decision-makers;
  c) supporting the technical handling of an incident or crisis, including facilitating the sharing of technical solutions between Member States;
  d) supporting public communication around the incident or crisis;
  e) testing the cooperation plans to respond to such incidents or crises.

# Market

## Cybersecurity Certification Framework

- preparing candidate European cybersecurity certification schemes
- assist the Commission in providing the secretariat to the European Cybersecurity Certification Group
- guidelines and developing good practices concerning the cybersecurity requirements of ICT products and services

## Standardisation

- facilitate establishment & take-up of EU & international standards for risk management and for the security of ICT products &services
- advice and guidelines related to the security requirements for OES and DSPs, as well as regarding already existing standards (NIS-D art. 19)

## Market Observatory

- analyses on trends of cybersecurity market (demand and supply sides)

# Knowledge, information & awareness

- Long term strategic analyses of cyber threats& incidents
- Analyses of emerging technologies

**Knowledge**

One stop shop portal of information from EU institutions, Agencies and bodies

**Information Hub**

- Compiling reports to provide guidance after big incidents
- Provide guidance on good practices for individual users
- Regular campaigns

**Awareness Raising**

# R&I, International cooperation

## R&I

- Advice on research needs &priorities
- Participate, if delegated by Commission, in implementation of R&I programmes or as beneficiary

## International

- observer in the organisation of international exercises
- facilitating, upon request of Commission, the exchange of best practices
- providing, upon request, the Commission with expertise

# 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

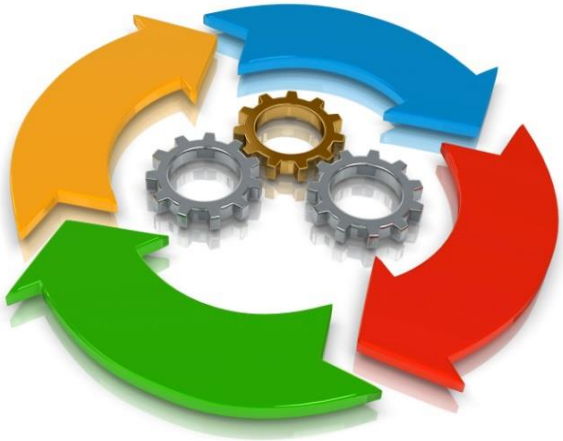
**Current landscape**

  - emergence of separate national initiatives lacking mutual recognition (e.g. France, UK, Germany, Netherlands, Italy)

  - SOG-IS MRA successful but
    - limited membership (13 MSs)
    - costs and duration not suitable for all market needs

# Our proposal

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



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

*…that are **valid across the EU***

# 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

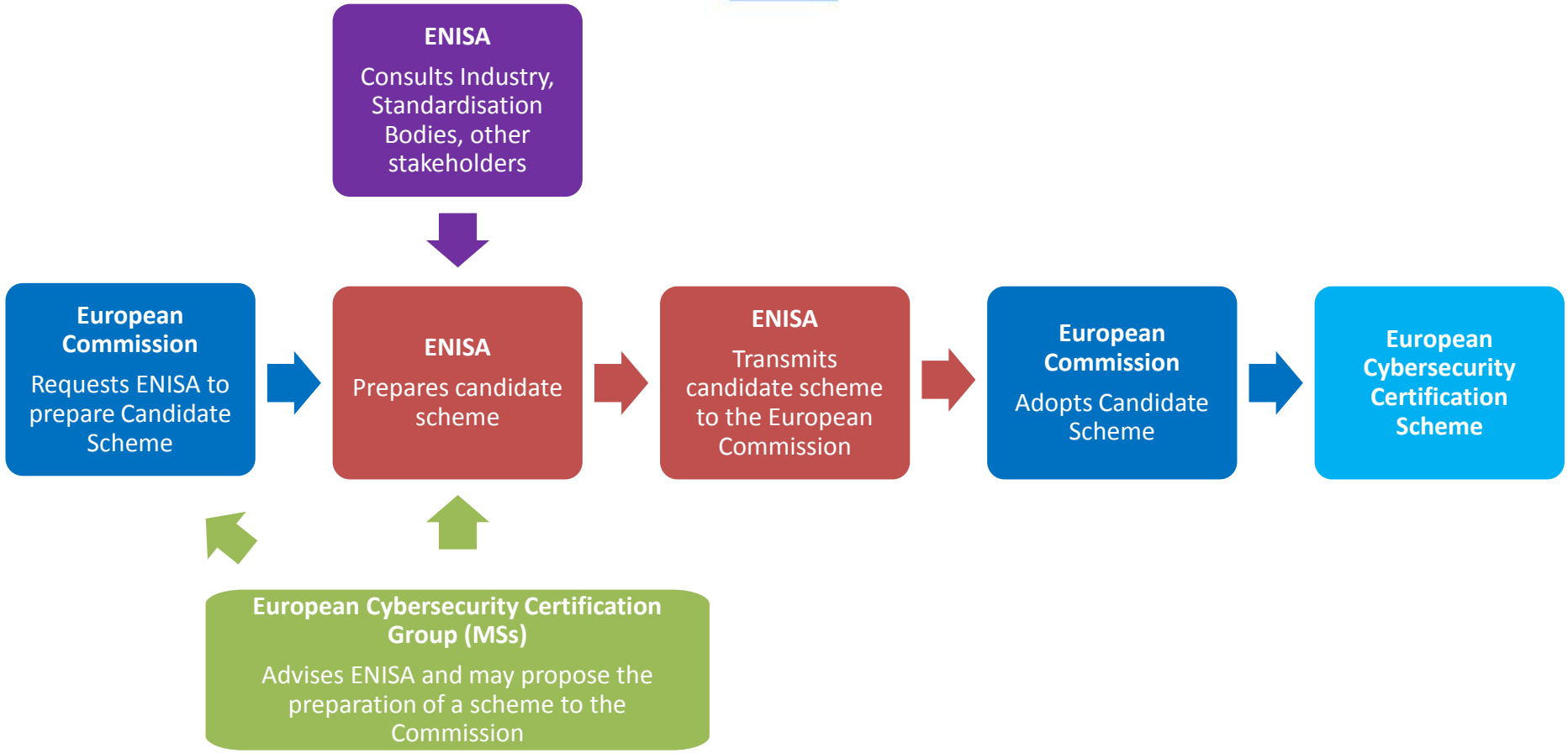
*…As end-users of digital solutions, governments would rely on an institutional framework to identify and express priority areas needing ICT security certification.*

# …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*

## Core elements (i)

- One EU Cybersecurity Certification Framework, **many** schemes.
- Tailored schemes specifying:
  i. scope - product/service category
  ii. evaluation criteria and security requirements
  iii. assurance level
- Resulting Certificates from European schemes are valid across all Member States.
- Once a European scheme has been established:
  – Member States cannot introduce new national schemes with same scope
  – Existing national schemes covering same product/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 European Union law.
- The specified requirements of the scheme shall not contradict any applicable legal requirements, in particular requirements emanating from harmonised Union legislation.




# Overview Establishment of an EU Cybersecurity Certification Scheme

## Core elements (ii)

National Authorities and the 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
  - Member States notify the Commission of the accredited CABs for each EU scheme
- 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.

European Commission

# Blueprint

# Resilience through crisis management and rapid emergency response

# Recommendation: Coordinated response to large-scale cybersecurity incidents and crises

- Establish an EU Cybersecurity Crisis Response Framework
  - standard operating procedures
  - information sharing and cooperation protocols
  - "integrating the objectives and modalities of cooperation presented in the **Blueprint** following the guiding principles described therein".

- Ensure that National Crisis Management mechanisms adequately address cybersecurity incident response as well as provide necessary procedures for cooperation at EU level within the context of the EU Framework.

- Develop and adopt a common **taxonomy** and template for situational reports describing the technical causes and impacts of cybersecurity incidents.

- Test in the context of the CyberEurope exercises organised by ENISA. **CyberEurope 2018 presents a first such opportunity.**

# Blueprint – Core objectives

# Blueprint – Cooperation at all levels

## Technical

- Incident handling  during a cybersecurity crisis.
- Monitoring and surveillance of incident including continuous analysis of threats and risk.

## Operational

- Preparing decision-making at the political level.
- Coordinate the management of the cybersecurity crisis (as appropriate).
- Assess the consequences and impact at EU level and propose possible mitigating actions.

## Political / Strategic

- Strategic and political management of both cyber and non-cyber aspects of the crisis including measures under the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities

# A cybersecurity competence network with a European Cybersecurity Research and Competence Centre

## Reinforcing EU's cybersecurity technologic capabilities and skills


## Idea in a nutshell

- Builds on the work of Member States and the cPPP to:
- Stimulate development and deployment of technology in cybersecurity
- Give impetus to innovation and competitiveness of the EU industry on the global scene in the development of next-generation digital technologies (AI, quantum computing, block chain, secure digital identities)
- Support industry through testing and simulation to underpin the cybersecurity certification
- Complement skills development efforts at EU and national level
- In the second phase - stimulate synergies between civilian and defence markets that share common challenges

# Horizon Prize

***Seamless authentication for all***

*Award for the best and most innovative authentication solutions*

***Compete, Innovate & Win - €4 million***

*Contest is open until 27 September 2018 !*

Horizon **Prize**

Seamless authentication for all



***www.ec.europa.eu/horizonprize-authentication***
***& cnect-a2-prize@ec.europa.eu***

# Thank you for your attention!