THE EU CYBERSECURITY AGENCY

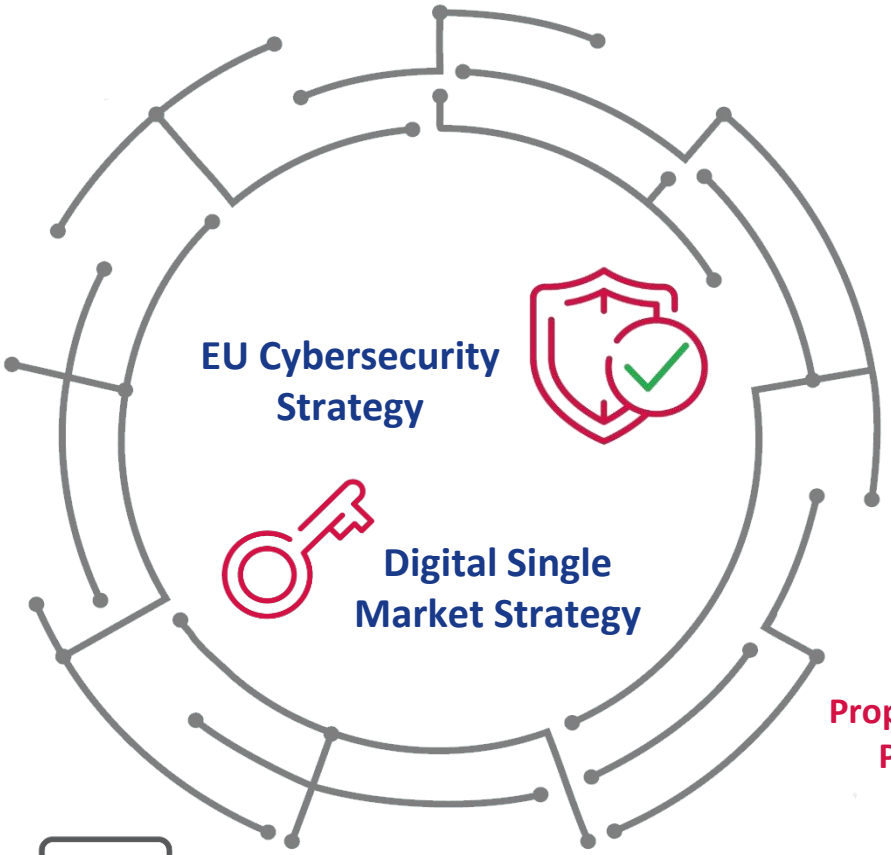
ENISA in the EU Cybersecurity Certification Framework

Sławek Górniak

IHE Europe Symposium
Rennes, France

09 | 04 | 2019

POLICY DEPENDENCIES



Network and Information Security Directive

eIDAS Regulation

Payment Services Directive 2

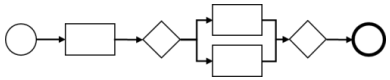
General Data Protection Regulation

Proposal for a Regulation on Privacy and Electronic Communications

Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry

FAST FORWARD INTO THE FUTURE

Present



It is challenging to identify if a product/service/process is secure

Uneven comparison in the absence a common cybersecurity certification framework

Future

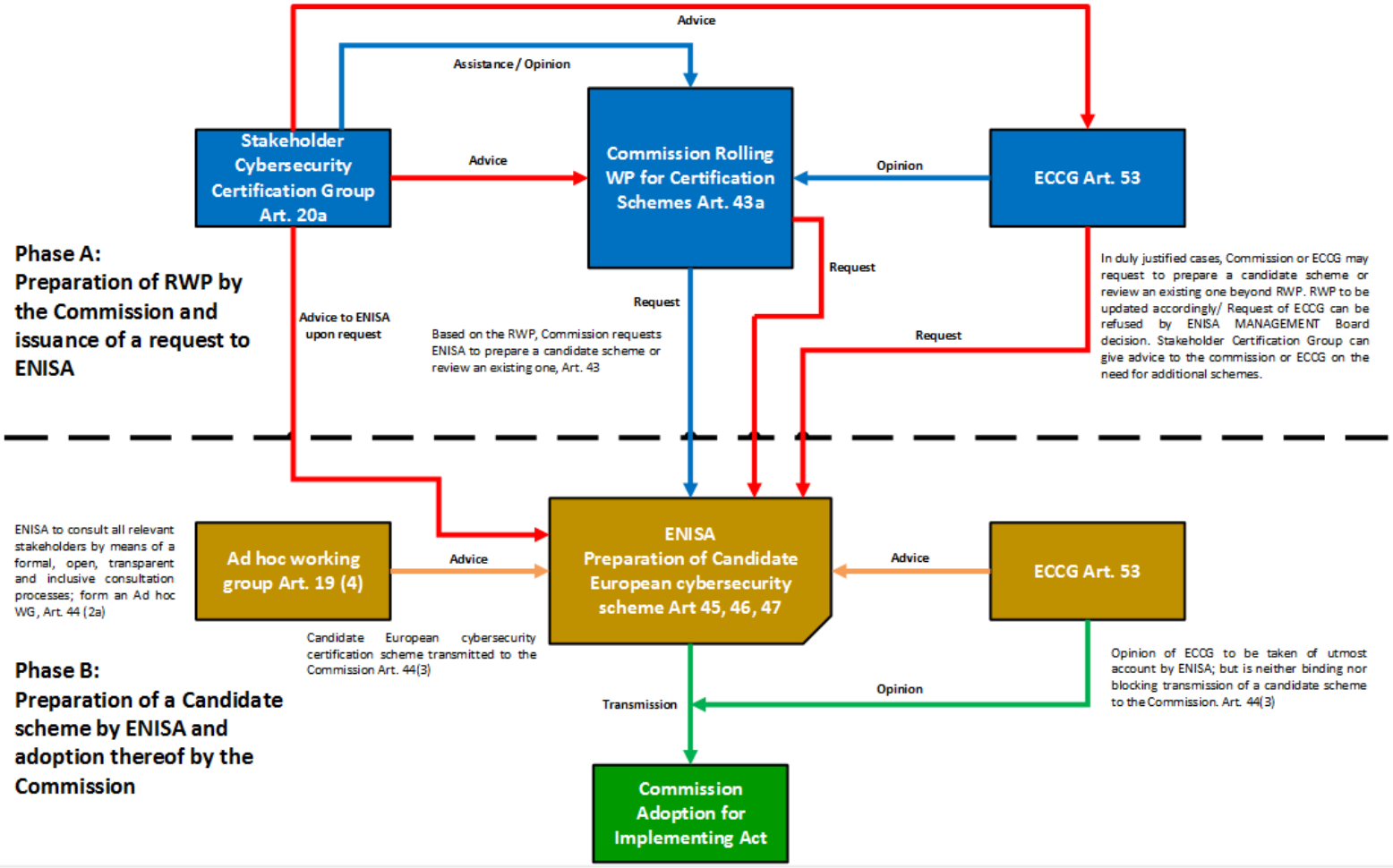
Straightforward comparison by identifying security specifications

Certification based on a harmonized framework

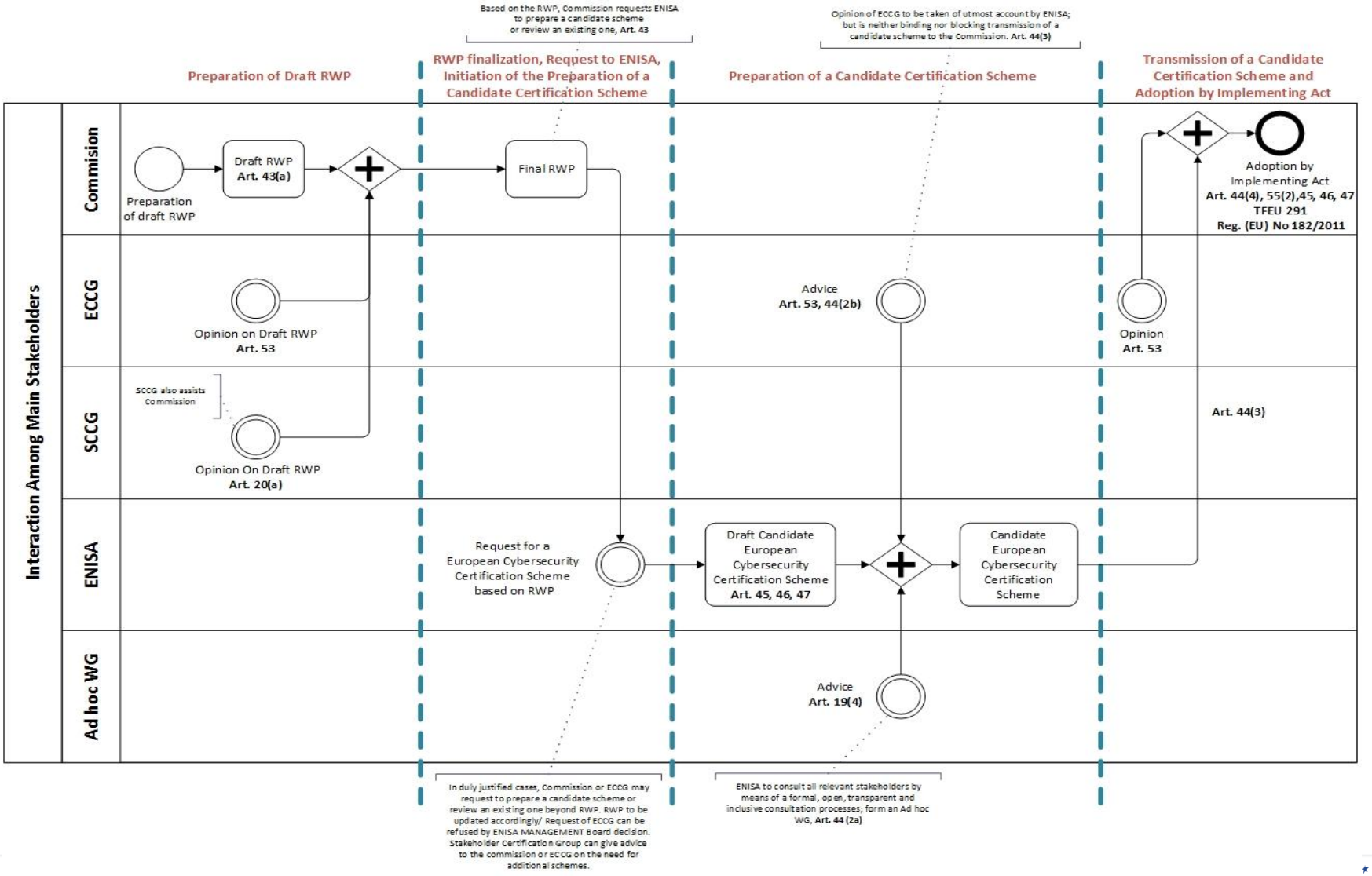
GOALS OF THE CSC FRAMEWORK

- **Addresses market fragmentation**
  - Products, services, processes
- **A risk-based approach for voluntary certification**
  - EU declaration of conformity
- **Defined assurance levels (Basic, Substantial, High)**
- **Role for Member States**
  - Propose the drafting of a candidate scheme
  - Involvement through European Cybersecurity Certification Group (composed of national certification supervisory authorities)
  - Involved in the adoption of an implementing act
- **Tasks outlined as per Regulation (EU) 765/2008 on accreditation and market surveillance**

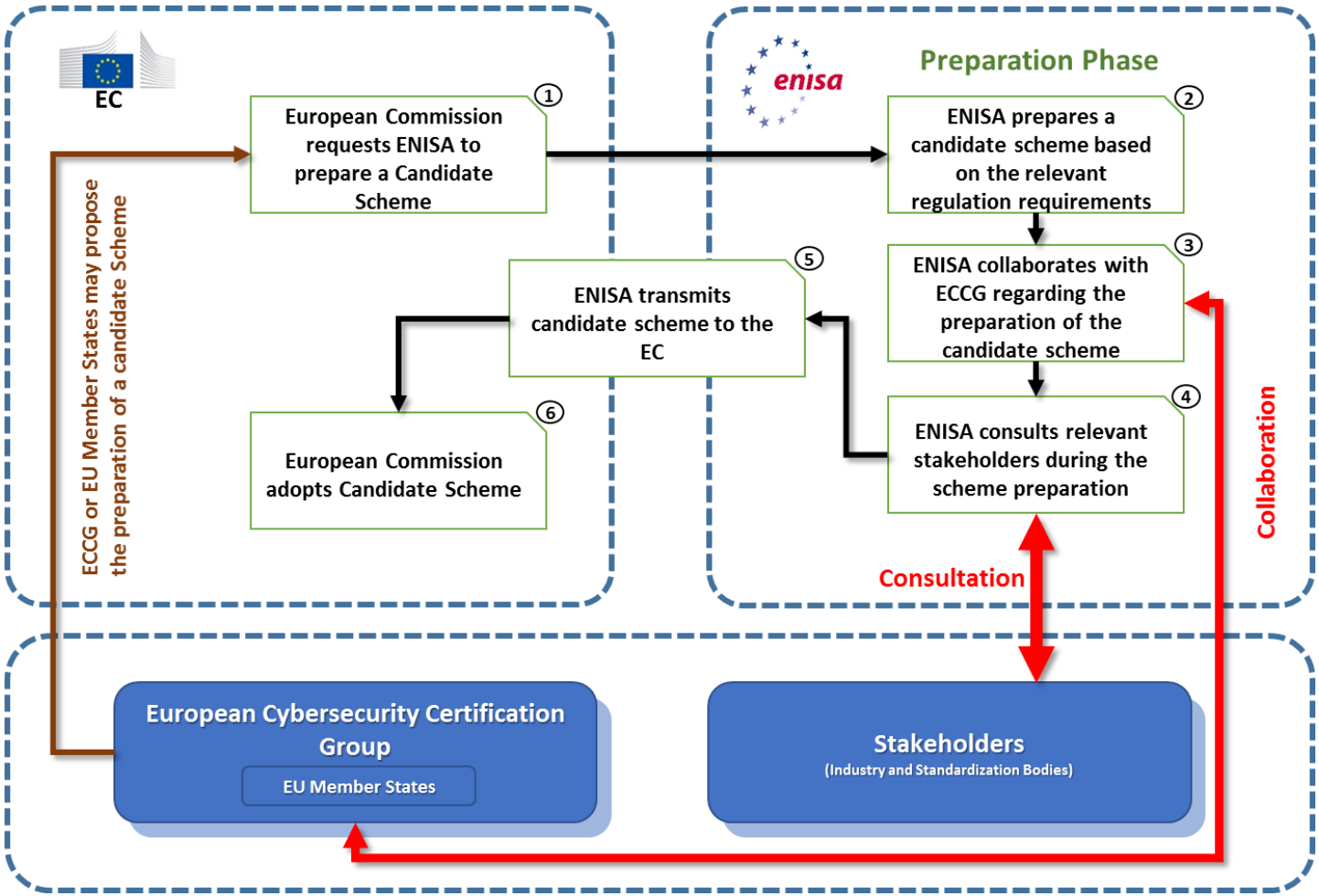
INTERACTION AMONG MAIN STAKEHOLDERS



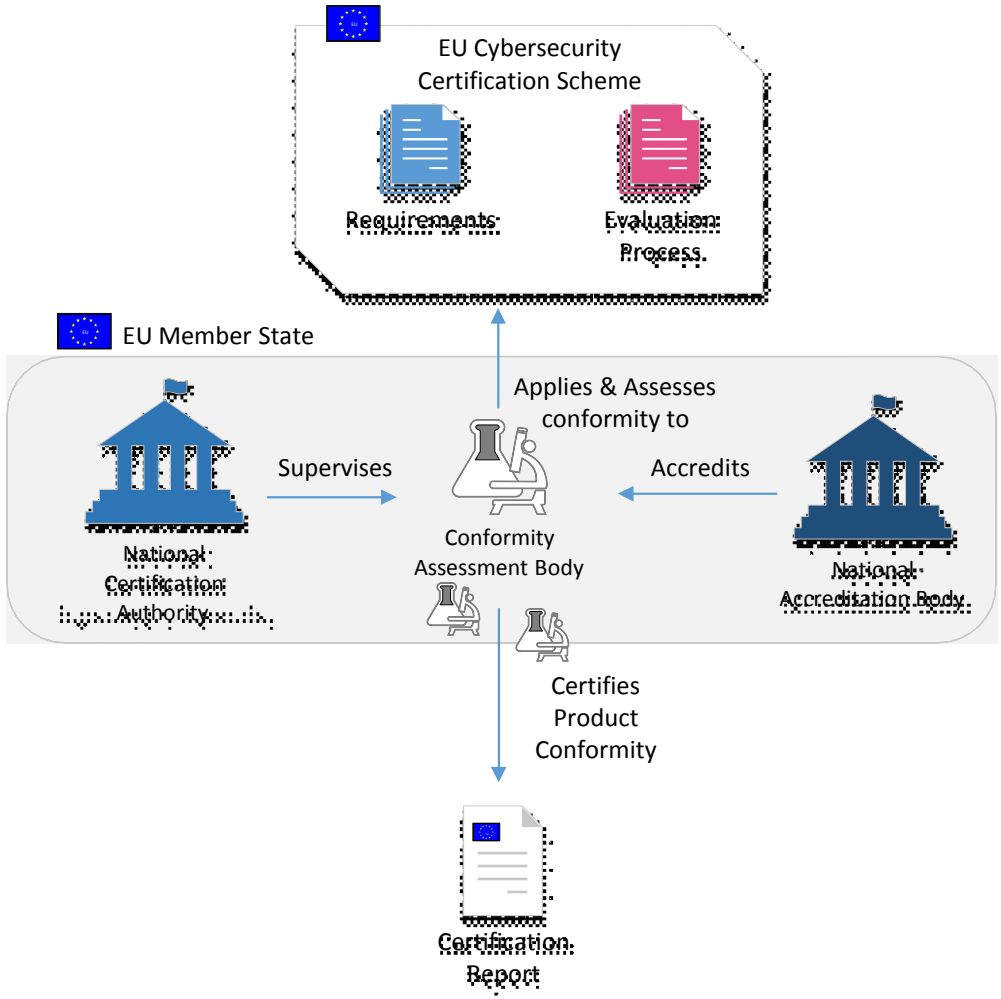
STAKEHOLDERS' PROCESS



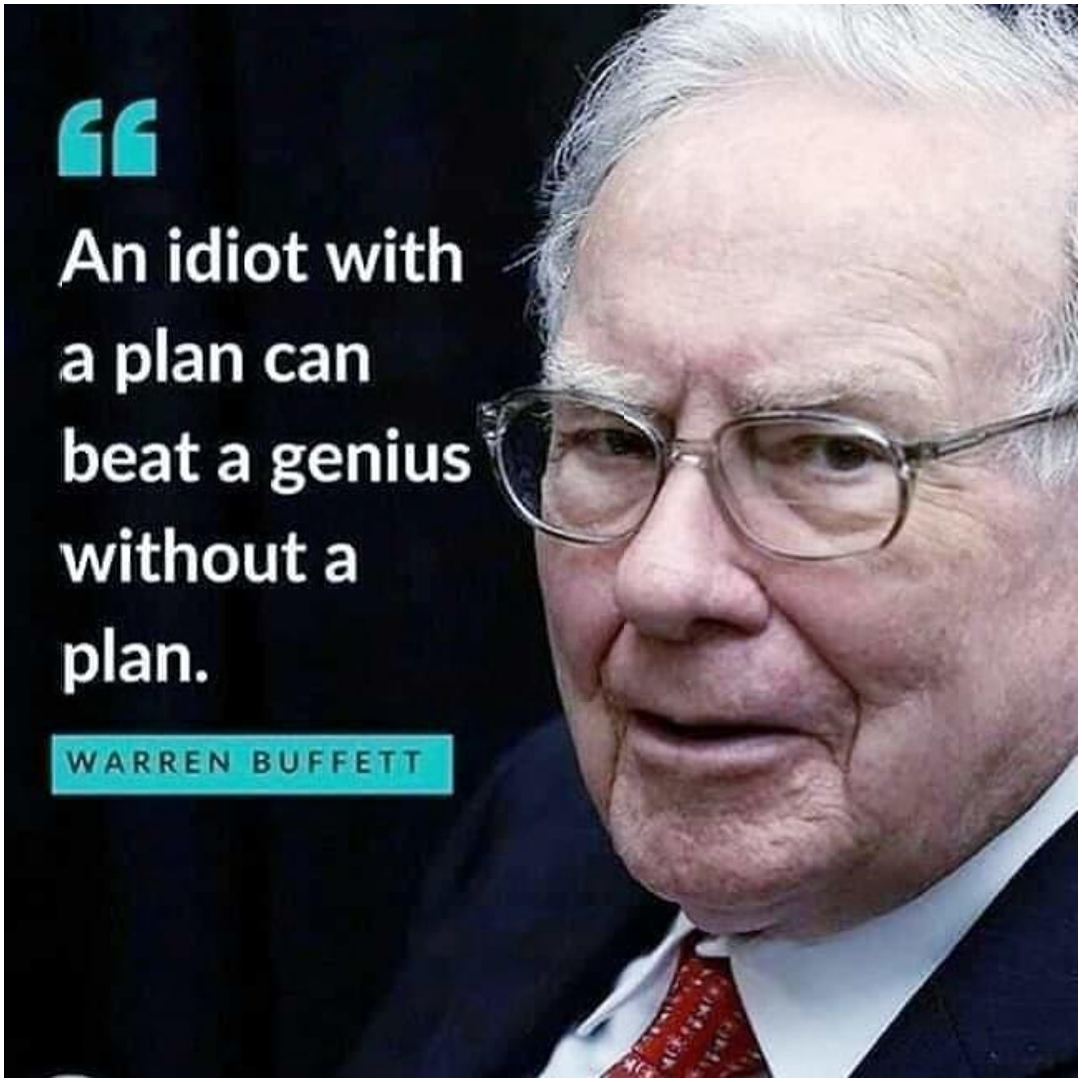
ROLLING OUT SCHEMES…



… AND PUTTING THEM TO WORK



SO, WHAT'S THE PLAN?



ENISA DUTIES

To contribute to the emerging EU framework for the certification of products, services and processes

To draw up **certification schemes in line with the Cybersecurity Act** providing stakeholders with a sound service that adds value to the EU

Key outputs

- Drafts and finalised schemes for certification, in the meaning of the Cybersecurity Act
- Secretariat support (SCCG)
- Co-chair SCCG (w/ Commission)
- Support the Commission to Chair ECCG
- Advice on market aspects etc.

MOST URGENT ACTIONS

- **Governance of the framework**
  - Modalities of ECCG
  - Modalities of SCCG
  - Format and content of requests
  - Procedures of ad-hoc groups
- **Processes and systems**
  - Procedures for requests
  - Procedures for interaction with stakeholders
  - Internal processes
  - IT systems needed
- **Timeline**

CERTIFICATION OPPORTUNITIES IN THE HEALTHCARE SECTOR

- **Scope of certification**
- Semiconductors – chips used in medical equipment
- Medical devices – from small to sophisticated, IoMT
- Electronic services – IT systems, cloud

- **Security requirements**
- Security by design
- Privacy by design
- Operational measures
- Technical measures

- **Some conclusions**
- Final products using certified components
- Differences between IoT and IoMT
- Assessment of full traceability of manufacturing
- Safety prevails over security
- Confidentiality and integrity of data of utmost importance

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

info@enisa.europa.eu

www.enisa.europe.eu