State of Cybersecurity in the European Union

ITU Cyber Drill – ALERT for European Region

29 May 2019
Bucharest, Romania

Ioannis Askoxylakis
Cybersecurity Policy Officer
Unit H1: Cybersecurity Technology & Capacity Building
Directorate H: Digital Society, Trust and Cybersecurity
Directorate General for Communication Networks, Content & Technology
DG CONNECT
European Commission

European
Commission

STATE OF
THE UNION

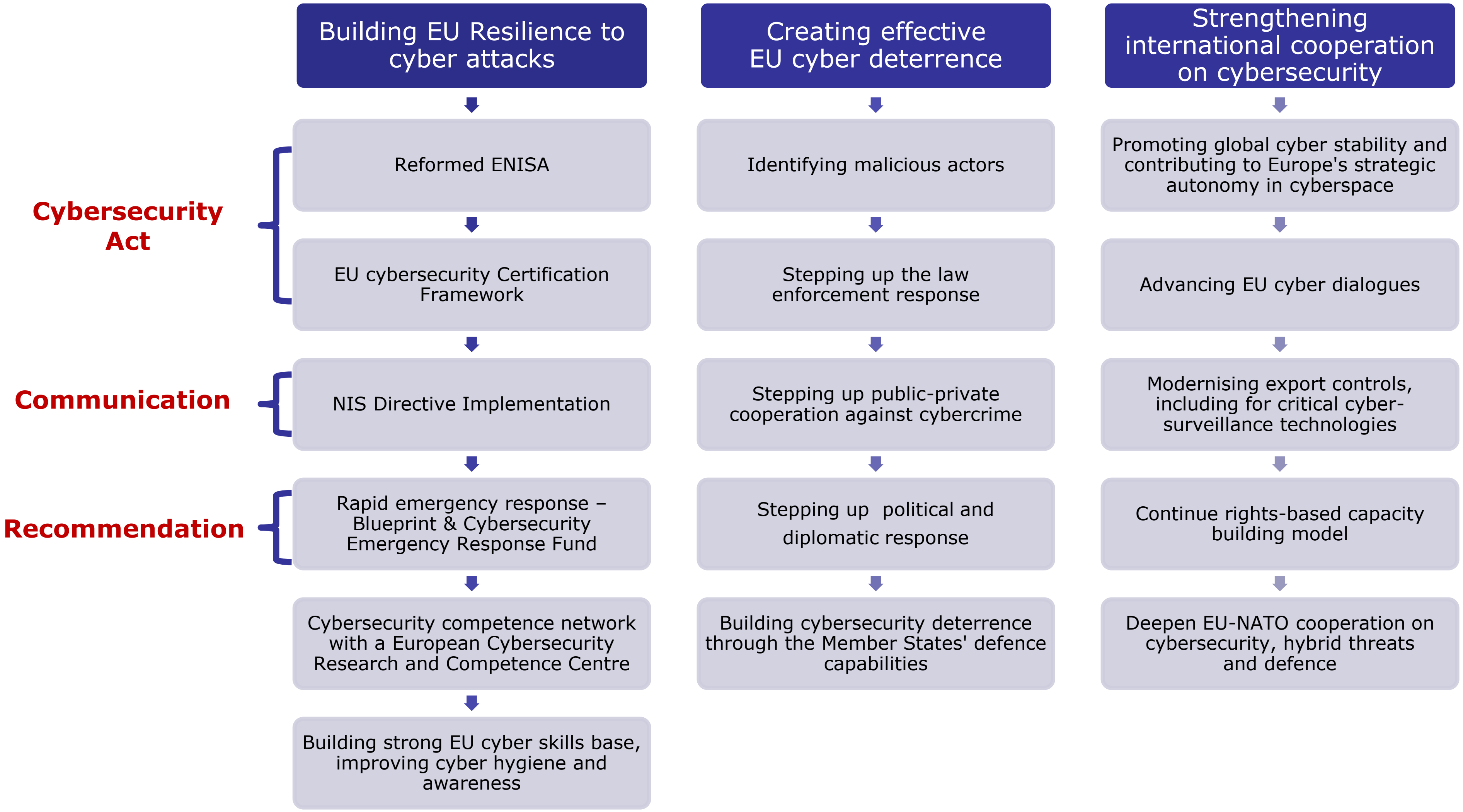
2018

Building strong cybersecurity in Europe

#SOTEU

‘Cyber-attacks know no borders, but our response capacity differs very much from one country to the other, creating loopholes where vulnerabilities attract even more the attacks. The EU needs more robust and effective structures to ensure strong cyber resilience and respond to cyber-attacks. We do not want to be the weakest links in this global threat.’

Jean-Claude Juncker, Tallinn Digital Summit, 29 September 2017



Cybersecurity Act

Communication

Recommendation

Building EU Resilience to cyber attacks

- Reformed ENISA
- EU cybersecurity Certification Framework
- NIS Directive Implementation
- Rapid emergency response – Blueprint & Cybersecurity Emergency Response Fund
- Cybersecurity competence network with a European Cybersecurity Research and Competence Centre
- Building strong EU cyber skills base, improving cyber hygiene and awareness

Creating effective EU cyber deterrence

- Identifying malicious actors
- Stepping up the law enforcement response
- Stepping up public-private cooperation against cybercrime
- Stepping up political and diplomatic response
- Building cybersecurity deterrence through the Member States' defence capabilities

Strengthening international cooperation on cybersecurity

- Promoting global cyber stability and contributing to Europe's strategic autonomy in cyberspace
- Advancing EU cyber dialogues
- Modernising export controls, including for critical cyber-surveillance technologies
- Continue rights-based capacity building model
- Deepen EU-NATO cooperation on cybersecurity, hybrid threats and defence

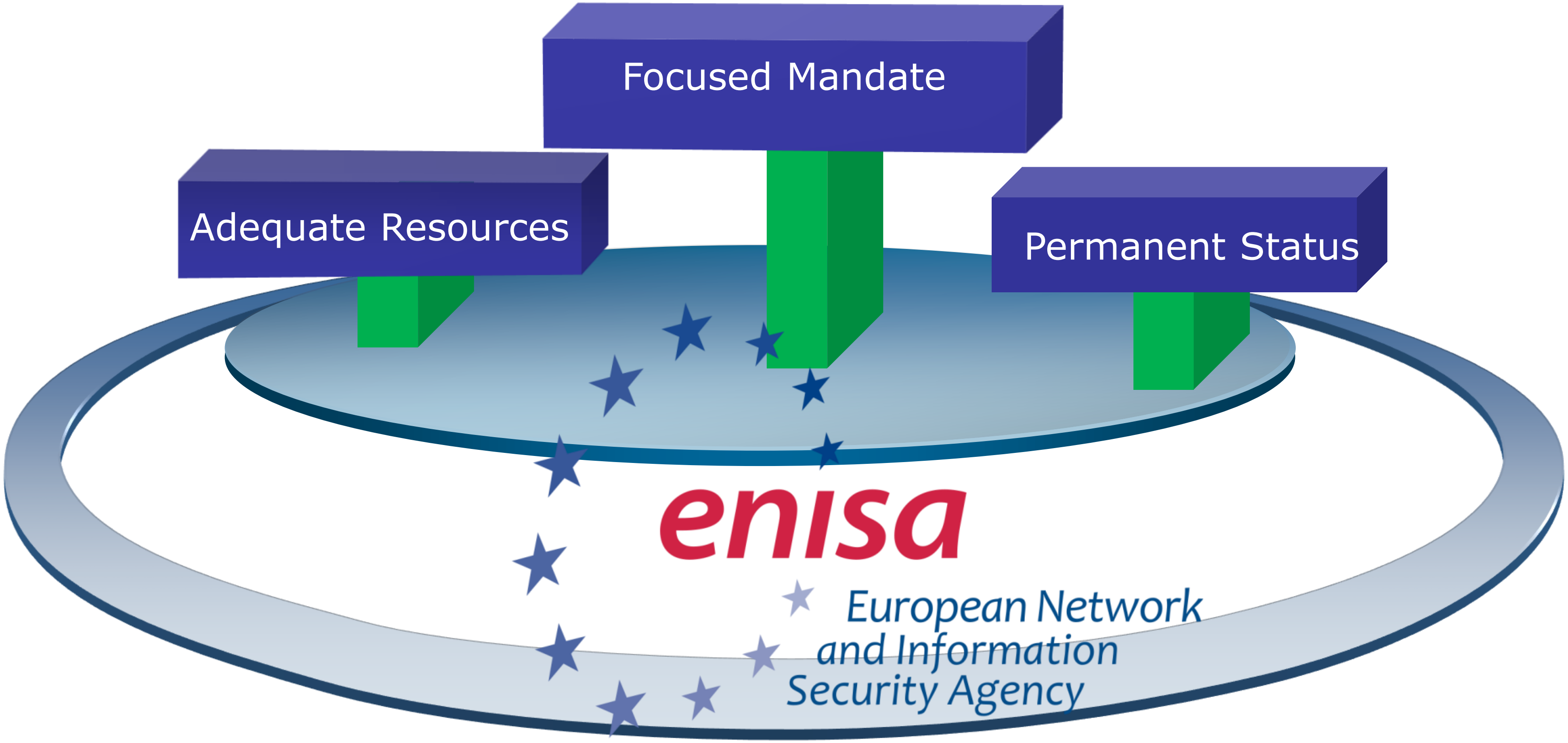
European Commission

EU Cybersecurity Act

Towards a reformed EU Cybersecurity Agency

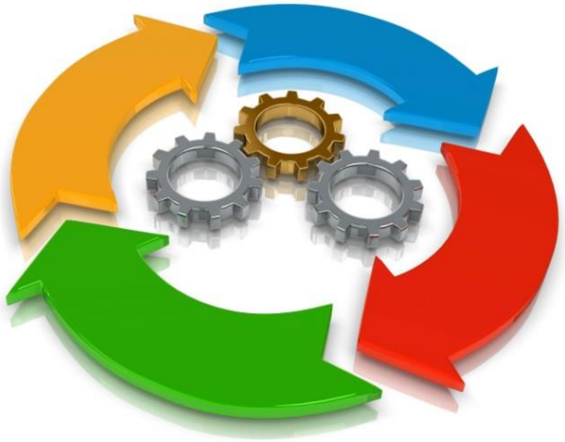
and reinforcing the cybersecurity single market in the EU

What's new with the new proposal?



Cybersecurity Certification

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



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

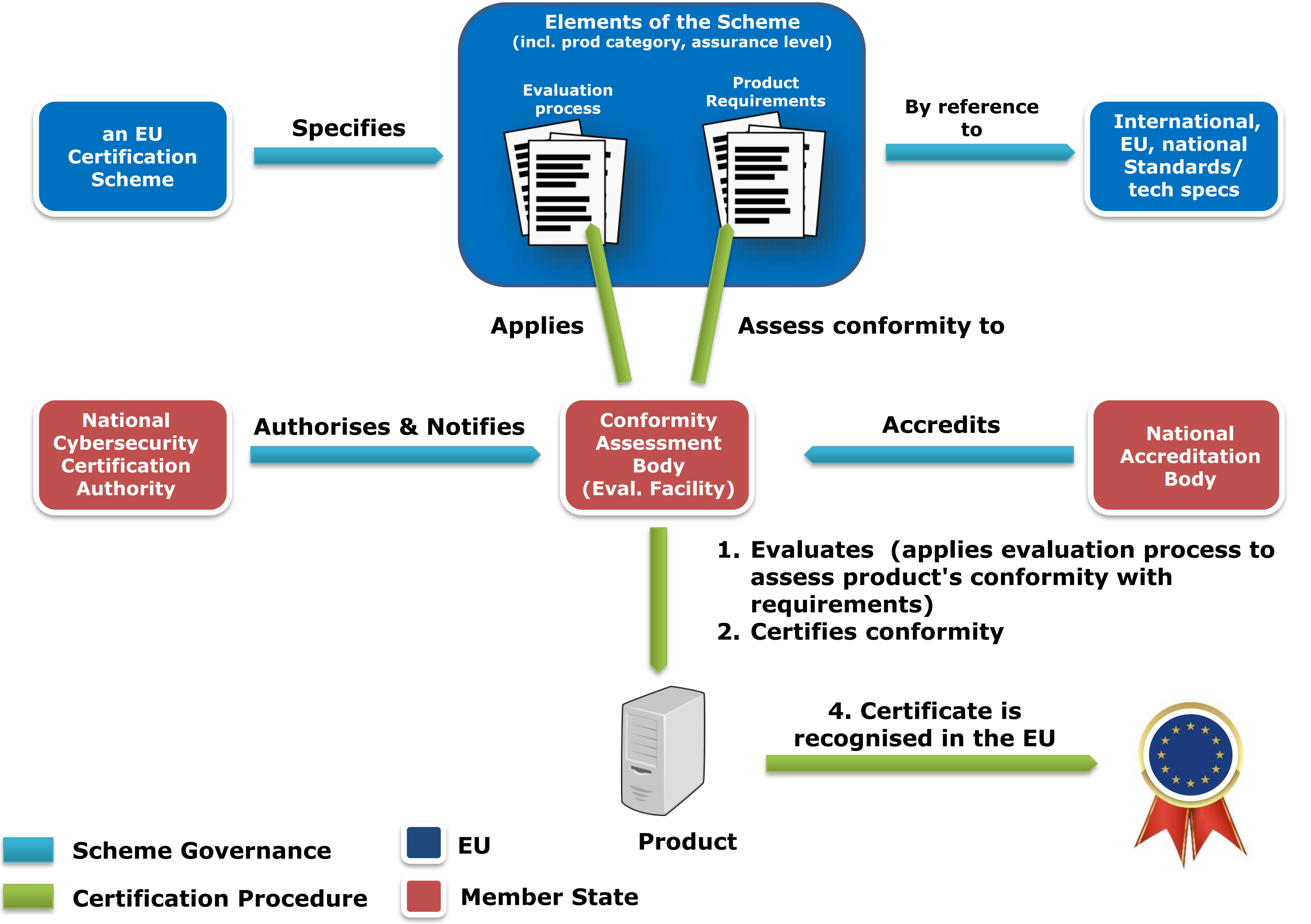
*…that are **valid across the EU***

The EU Cybersecurity Certification Framework

Cybersecurity Certification Schemes

- Security Objectives
- Assurance levels: Basic, Substantial, High
- Elements of a cybersecurity certification scheme include:
  - Scope - product/service or category(ies) thereof
  - references to the international, European or national standards and to technical specifications
  - one or more assurance levels
- conditions for the mutual recognition of certification schemes with third countries;

European Cybersecurity Certification Scheme (Basic, Substantial)



an EU Certification Scheme

Specifies

Elements of the Scheme (incl. prod category, assurance level)

Evaluation process

Product Requirements

By reference to

International, EU, national Standards/ tech specs

Applies

Assess conformity to

National Cybersecurity Certification Authority

Authorises & Notifies

Conformity Assessment Body (Eval. Facility)

Accredits

National Accreditation Body

1. Evaluates (applies evaluation process to assess product's conformity with requirements)
2. Certifies conformity

Product

4. Certificate is recognised in the EU

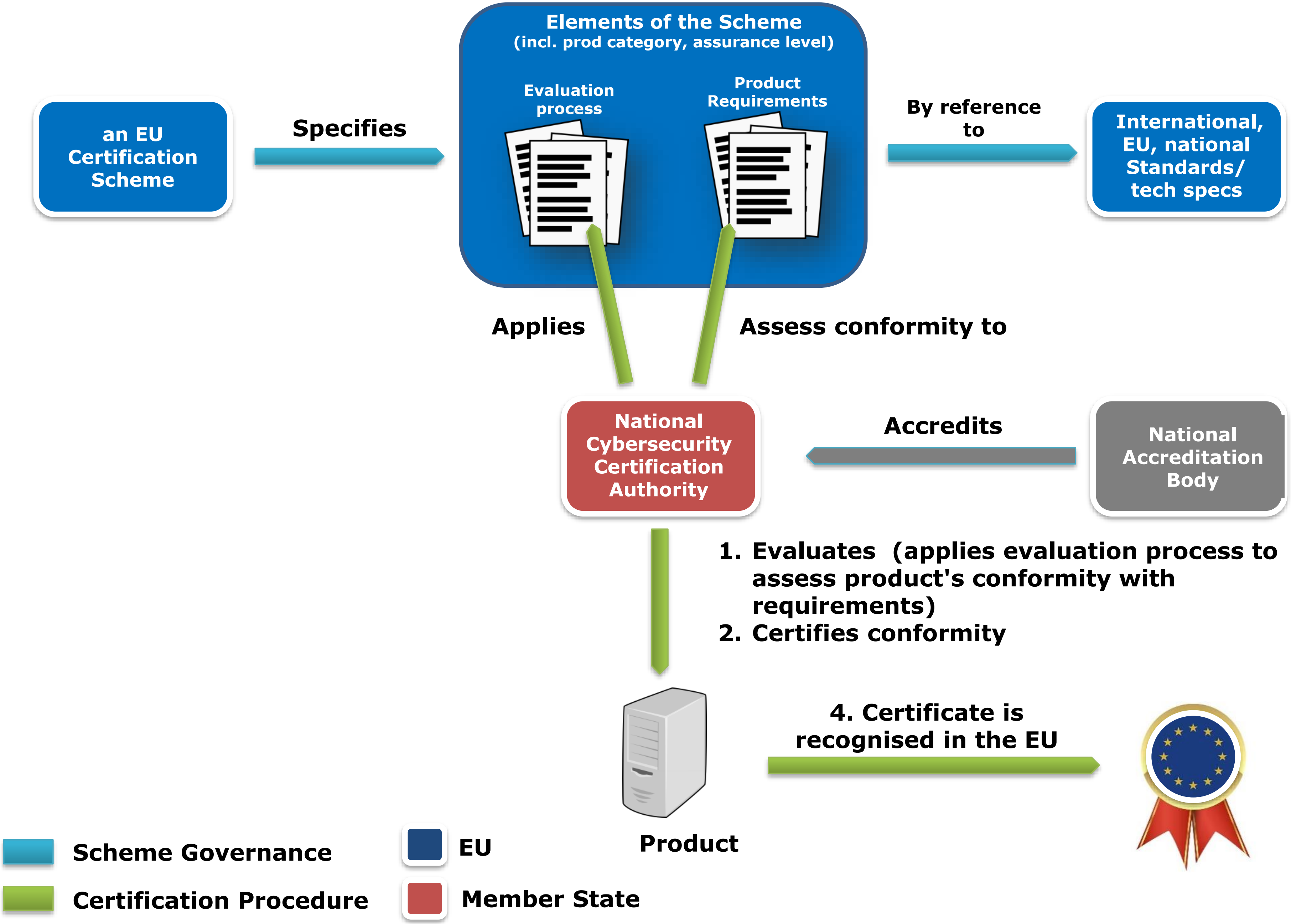
Scheme Governance

Certification Procedure

EU

Member State

European Cybersecurity Certification Scheme (High)



an EU Certification Scheme

Specifies

Elements of the Scheme
(incl. prod category, assurance level)

Evaluation process

Product Requirements

By reference to

International, EU, national Standards/ tech specs

Applies

Assess conformity to

National Cybersecurity Certification Authority

Accredits

National Accreditation Body

1. Evaluates (applies evaluation process to assess product's conformity with requirements)
2. Certifies conformity

Product

4. Certificate is recognised in the EU

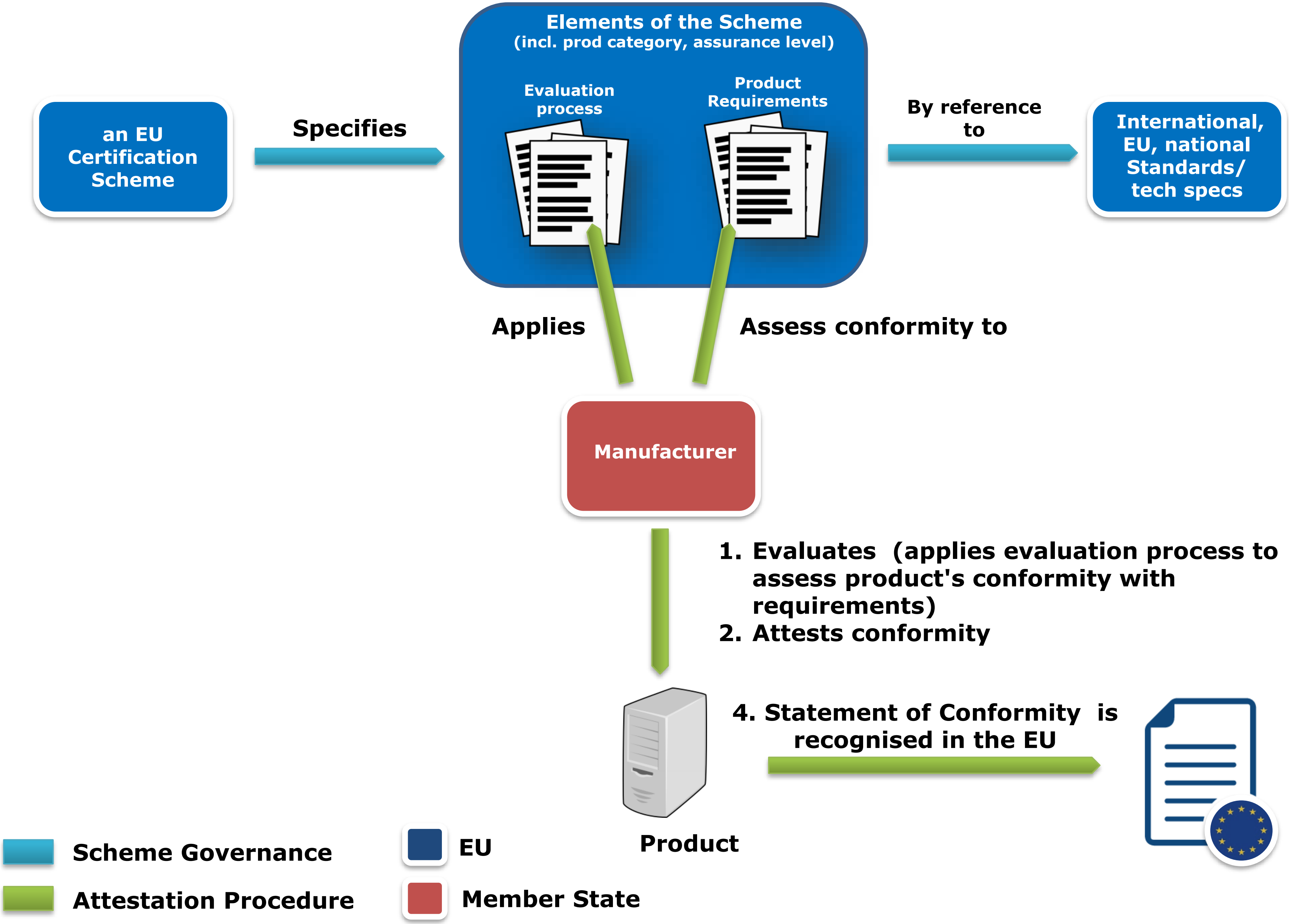
🟦 Scheme Governance

🟩 Certification Procedure

🟦 EU

🟥 Member State

Conformity self-assessment (AL Basic only)



an EU Certification Scheme

Specifies

Elements of the Scheme
(incl. prod category, assurance level)

Evaluation process

Product Requirements

By reference to

International, EU, national Standards/ tech specs

Applies

Assess conformity to

Manufacturer

1. Evaluates (applies evaluation process to assess product's conformity with requirements)
2. Attests conformity

Product

4. Statement of Conformity is recognised in the EU

🟦 Scheme Governance

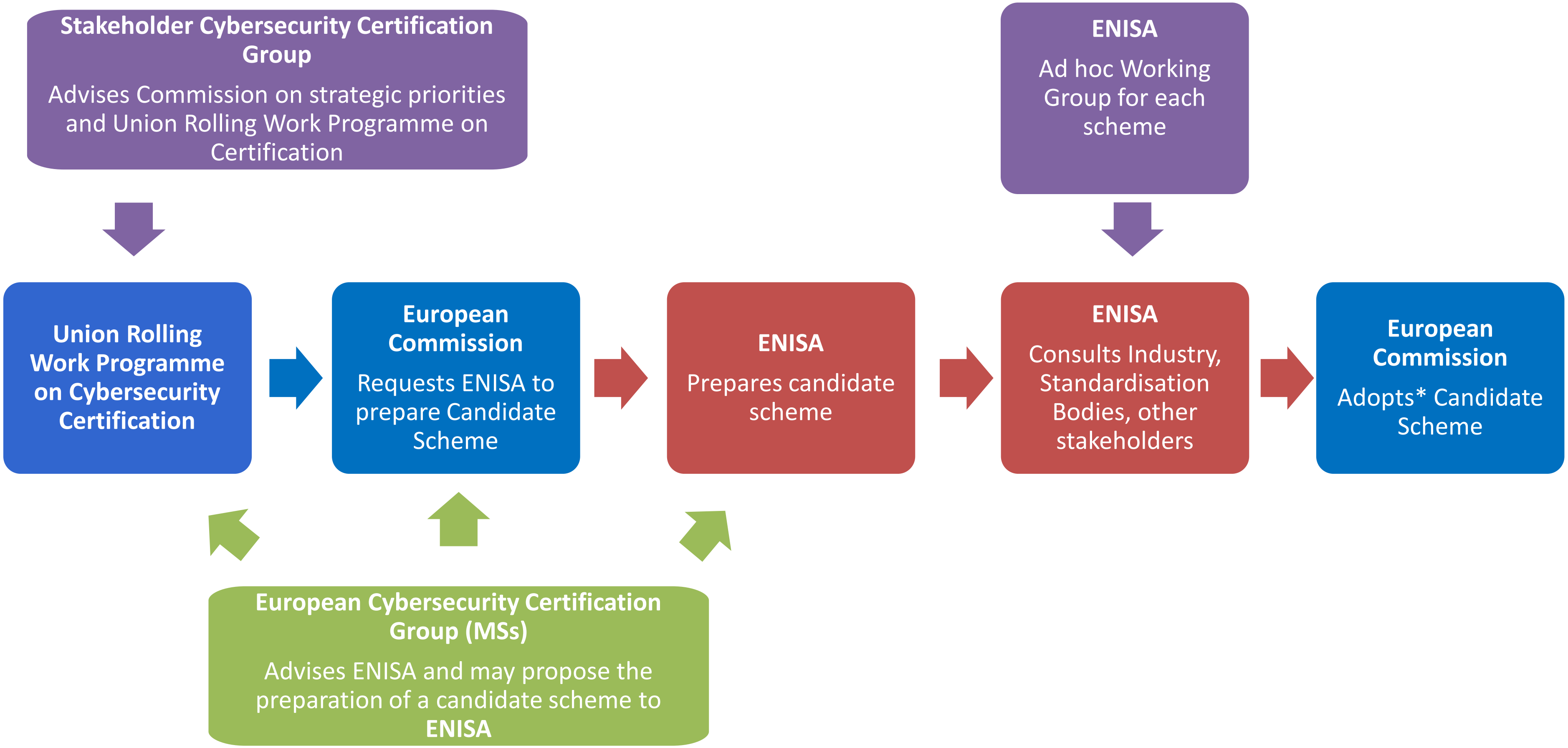
🟩 Attestation Procedure

🟦 EU

🟥 Member State

The EU Cybersecurity Certification Framework

The lifecycle of a European Cybersecurity Certification Scheme



Stakeholder Cybersecurity Certification Group

Advises Commission on strategic priorities and Union Rolling Work Programme on Certification

ENISA

Ad hoc Working Group for each scheme

Union Rolling Work Programme on Cybersecurity Certification

European Commission

Requests ENISA to prepare Candidate Scheme

ENISA

Prepares candidate scheme

ENISA

Consults Industry, Standardisation Bodies, other stakeholders

European Commission

Adopts* Candidate Scheme

European Cybersecurity Certification Group (MSs)

Advises ENISA and may propose the preparation of a candidate scheme to **ENISA**

NIS Directive

NIS Directive: Main Features

GREATER CAPABILITIES

Member States have to improve their cybersecurity capabilities.

NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIS-RT)

NATIONAL NIS STRATEGY

NATIONAL NIS AUTHORITY

COOPERATION

Increased EU-level cooperation

EU MEMBER STATES COOPERATION GROUP (STRATEGIC)

EU MEMBER STATES; EUROPEAN COMMISSION; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

EMERGENCY TEAMS (CSIRTS) NETWORK (OPERATIONAL)

EU MEMBER STATES; CERT-EU; EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY

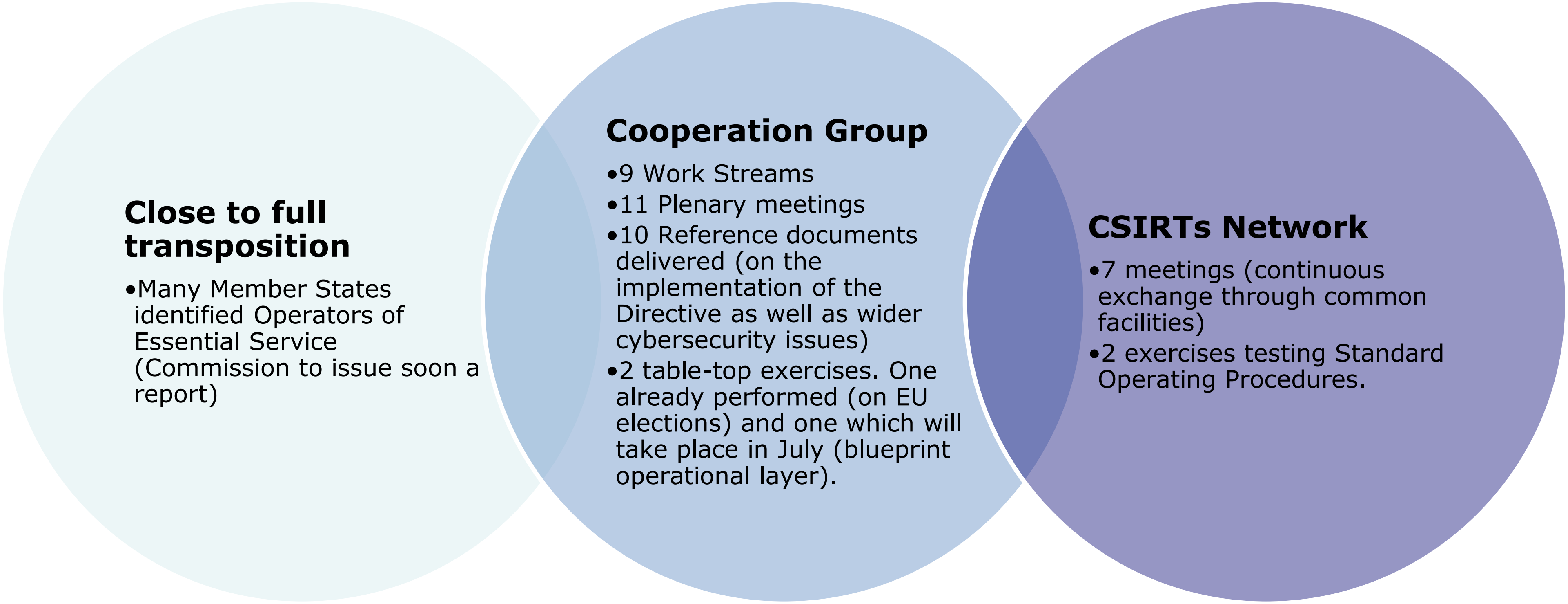
RISK MANAGEMENT

Operators of essential services and Digital Service Providers have to adopt risk management practices and notify significant incidents to their national authorities.

SECURITY MEASURES

NOTIFICATION OF MAJOR INCIDENTS

NIS implementation one year later



Close to full transposition

- Many Member States identified Operators of Essential Service (Commission to issue soon a report)

Cooperation Group

- 9 Work Streams
- 11 Plenary meetings
- 10 Reference documents delivered (on the implementation of the Directive as well as wider cybersecurity issues)
- 2 table-top exercises. One already performed (on EU elections) and one which will take place in July (blueprint operational layer).

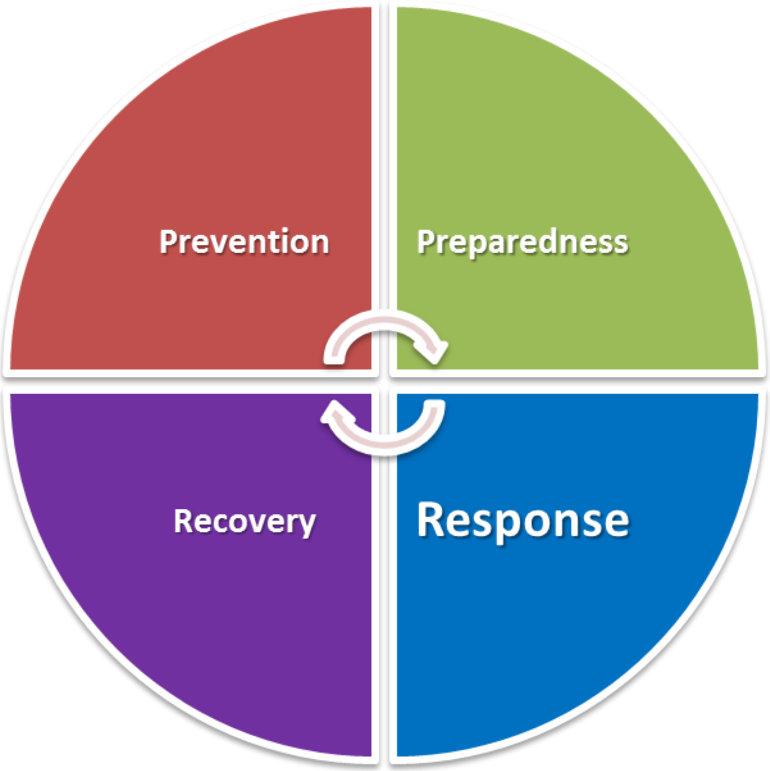
CSIRTs Network

- 7 meetings (continuous exchange through common facilities)
- 2 exercises testing Standard Operating Procedures.

Blueprint - coordinated response to large-scale cybersecurity incidents and crises

Resilience through crisis management and rapid emergency response

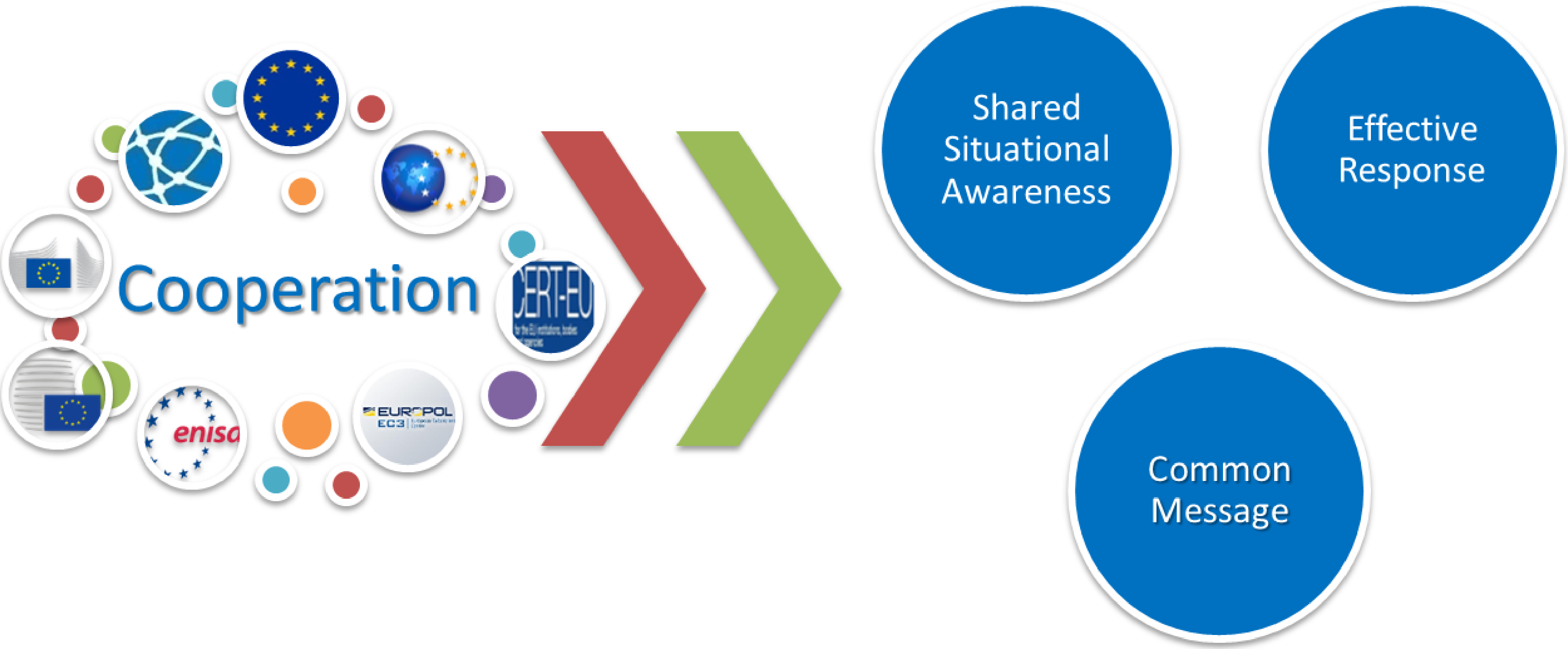
Blueprint - Response



Definition: large-scale cybersecurity incidents and crises

incidents which cause disruption too extensive for a concerned Member State to handle on its own or which affect two or more Member States or EU institutions with such a wide-ranging and significant impact of technical or political significance that they require timely policy coordination and response at Union political level

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.

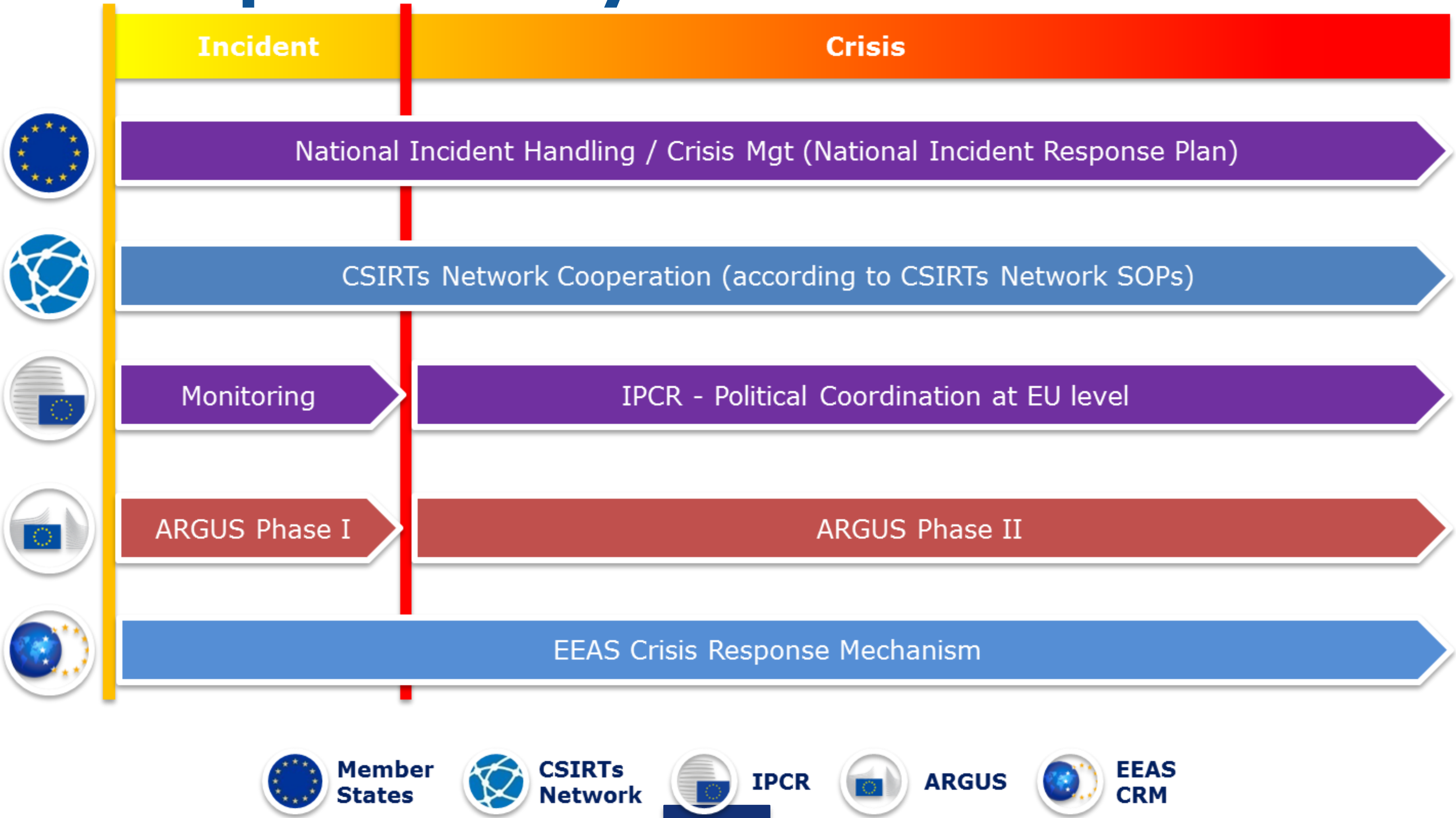
Operational

- 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

Blueprint – key mechanisms



Incident

Crisis

National Incident Handling / Crisis Mgt (National Incident Response Plan)

CSIRTs Network Cooperation (according to CSIRTs Network SOPs)

Monitoring

IPCR - Political Coordination at EU level

ARGUS Phase I

ARGUS Phase II

EEAS Crisis Response Mechanism

Member States

CSIRTs Network

IPCR

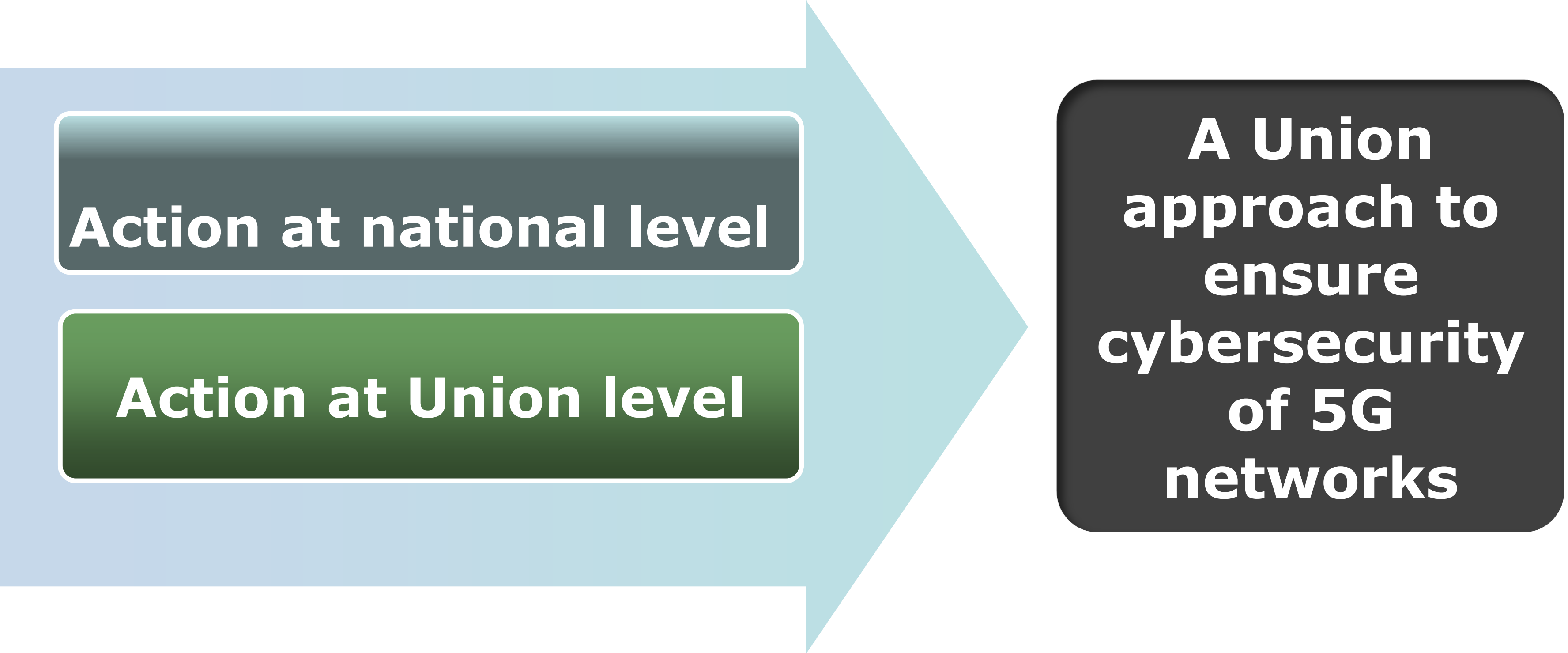
ARGUS

EEAS CRM

Commission Recommendation on Cybersecurity of 5G networks

European
Commission

Commission Recommendation on Cybersecurity of 5G networks – 26.03.2019

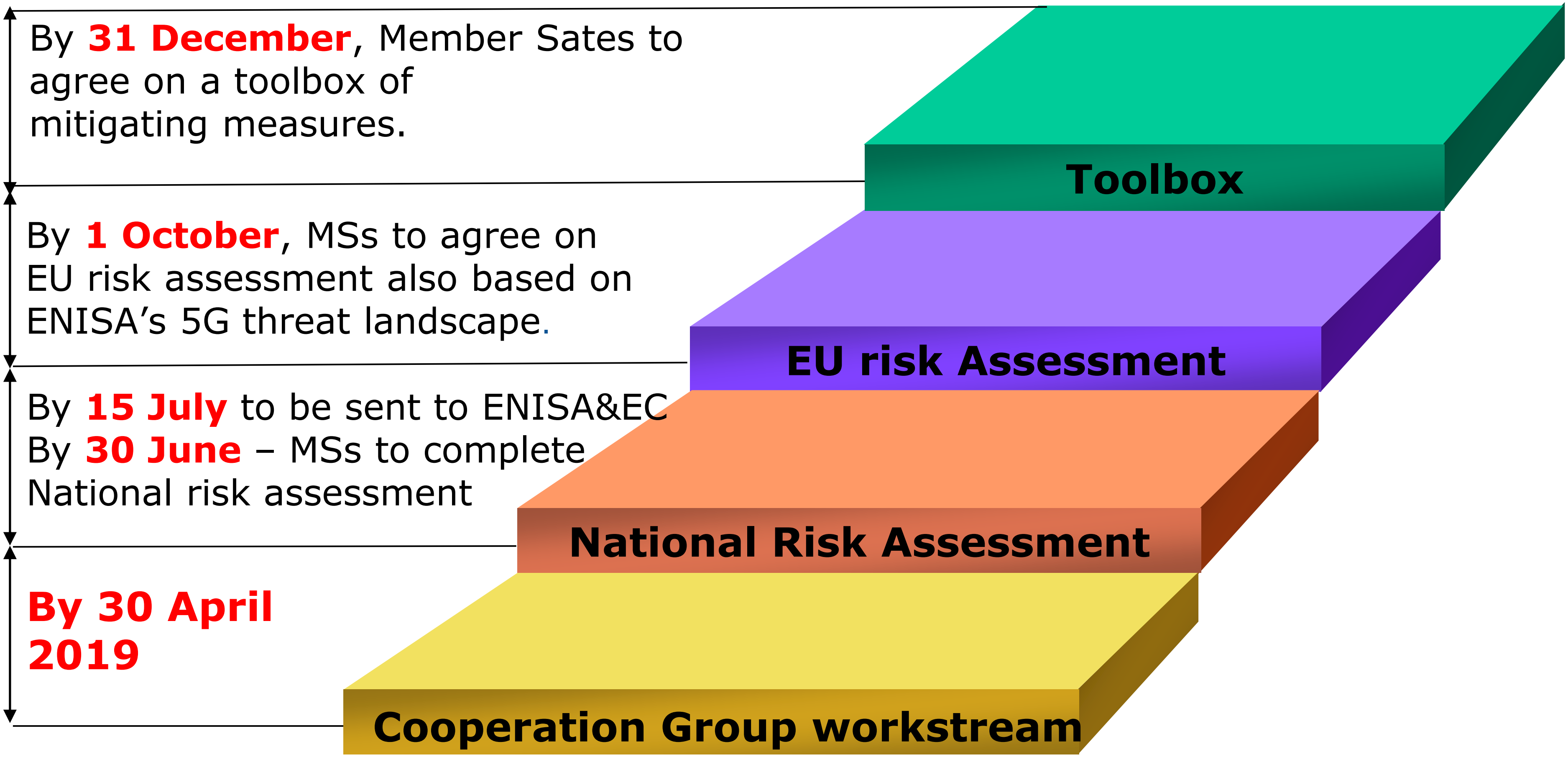


Action at national level

Action at Union level

A Union approach to ensure cybersecurity of 5G networks

Actions – short term



By **31 December**, Member Sates to agree on a toolbox of mitigating measures.

By **1 October**, MSs to agree on EU risk assessment also based on ENISA's 5G threat landscape.

By **15 July** to be sent to ENISA&EC
By **30 June** – MSs to complete National risk assessment

By 30 April 2019

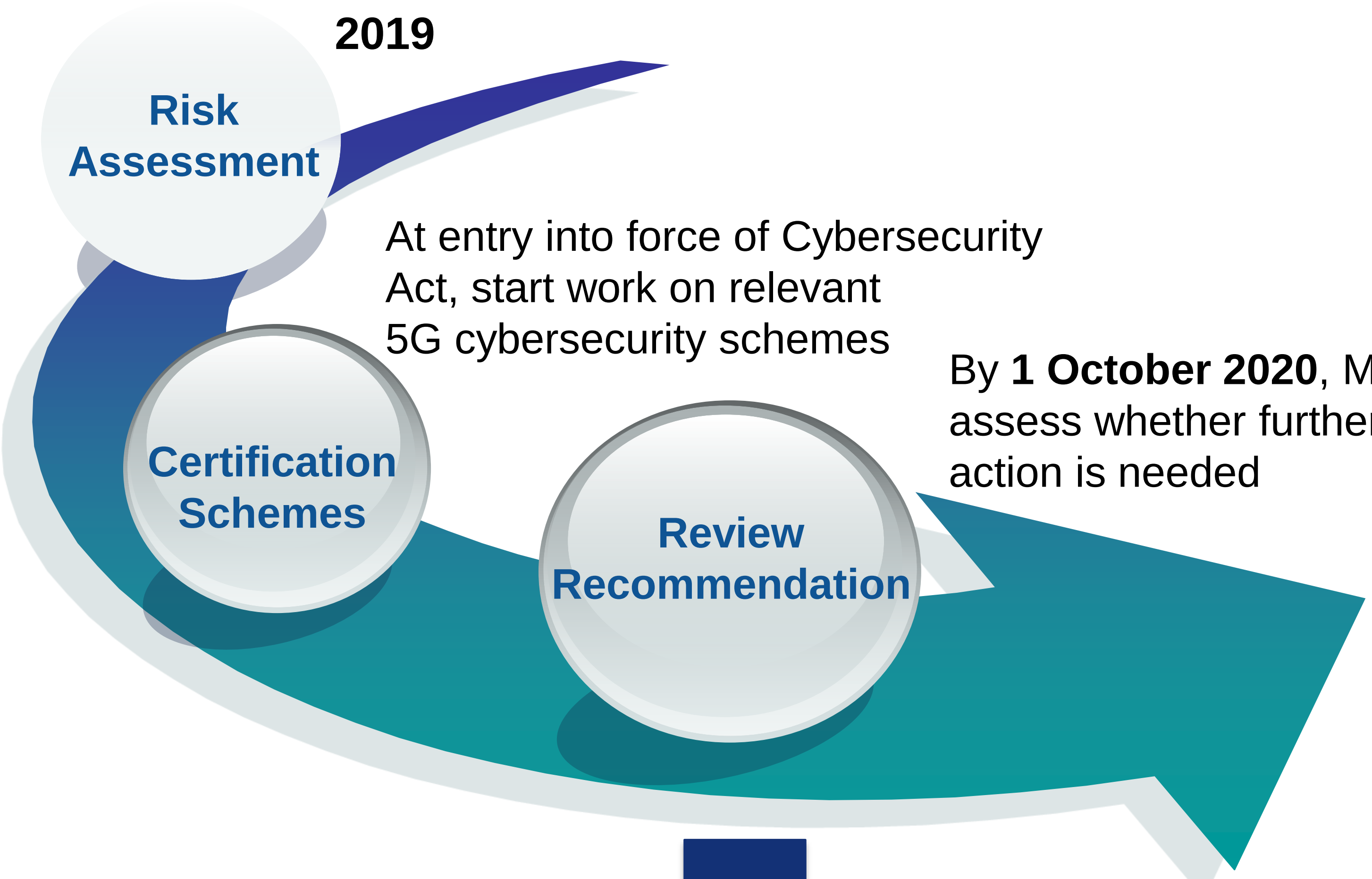
Toolbox

EU risk Assessment

National Risk Assessment

Cooperation Group workstream

Next steps – medium/longer term



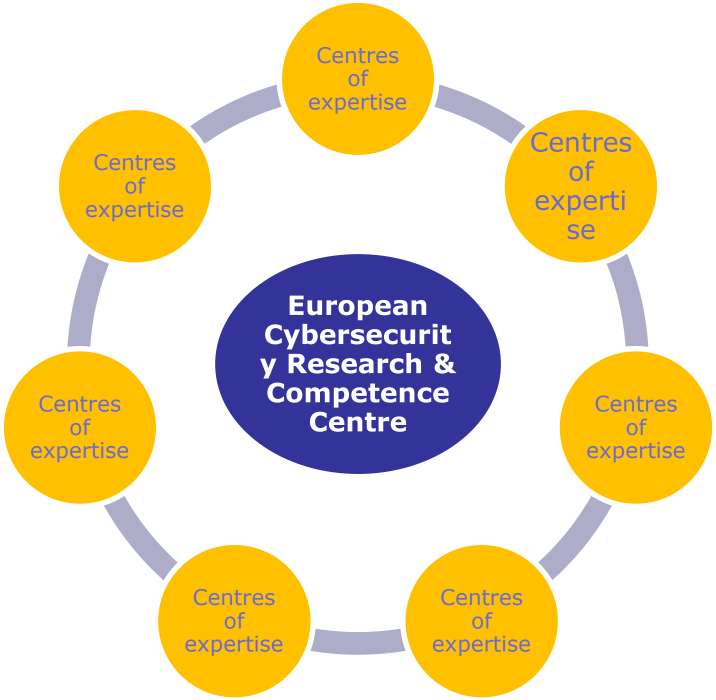
At entry into force of Cybersecurity Act, start work on relevant 5G cybersecurity schemes

By **1 October 2020**, MS to assess whether further action is needed

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

Reinforcing EU's cybersecurity technologic capabilities and skills

European Cybersecurity Industrial Technology and Research Competence Centre



European Cybersecurity Research & Competence Centre

Centres of expertise

Centres of expertise

Centres of expertise

Centres of expertise

Centres of expertise

Centres of expertise

Centres of expertise

Centre's Role:

Network coordination and support

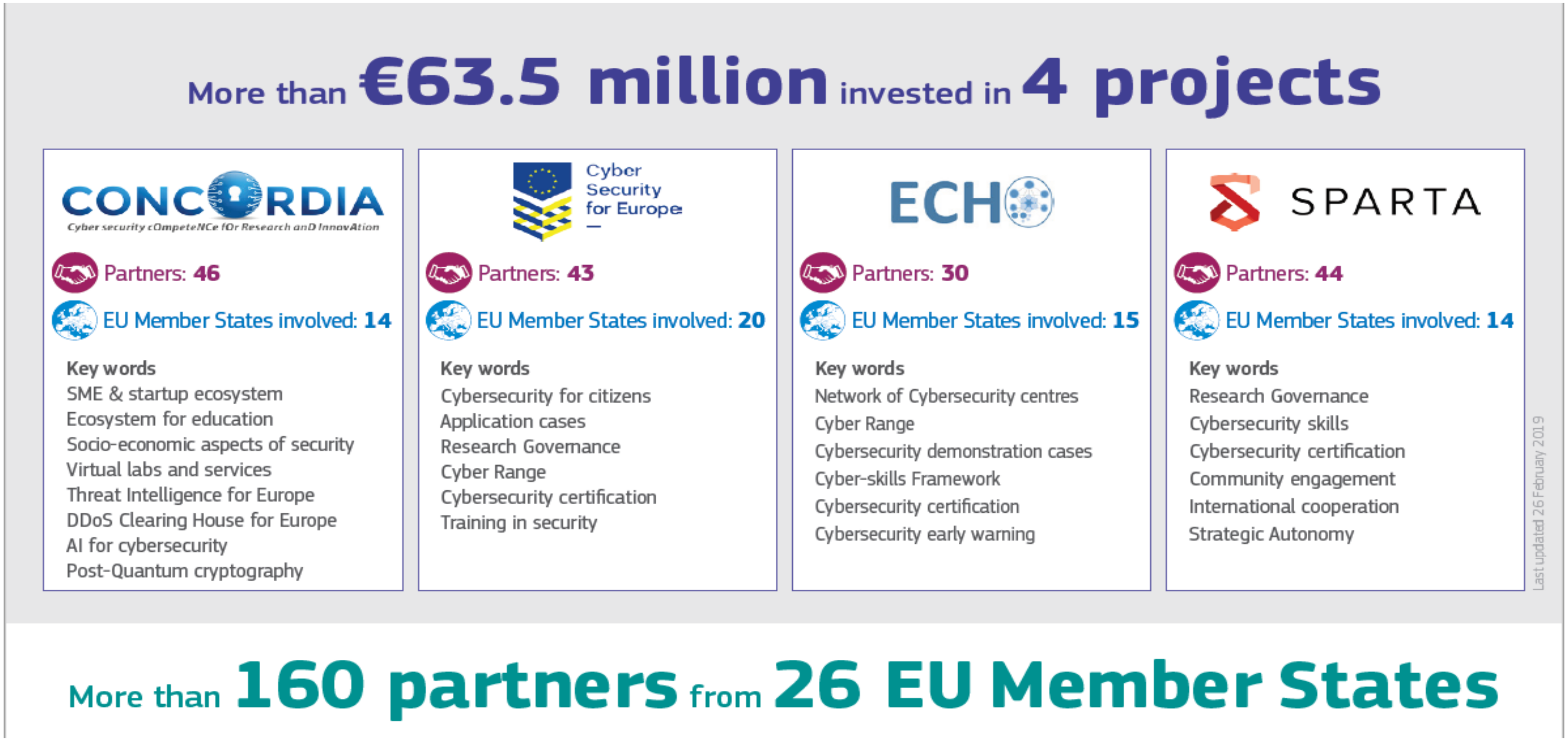
Research programming and implementation

Procurement

Ensuring synergies between civilian and defence spheres

European Commission

EU pilots to prepare the European Cybersecurity Competence Network



More than **€63.5 million** invested in **4 projects**

CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion

Partners: **46**
EU Member States involved: **14**

Key words
SME & startup ecosystem
Ecosystem for education
Socio-economic aspects of security
Virtual labs and services
Threat Intelligence for Europe
DDoS Clearing House for Europe
AI for cybersecurity
Post-Quantum cryptography

Cyber Security for Europe

Partners: **43**
EU Member States involved: **20**

Key words
Cybersecurity for citizens
Application cases
Research Governance
Cyber Range
Cybersecurity certification
Training in security

ECHO

Partners: **30**
EU Member States involved: **15**

Key words
Network of Cybersecurity centres
Cyber Range
Cybersecurity demonstration cases
Cyber-skills Framework
Cybersecurity certification
Cybersecurity early warning

SPARTA

Partners: **44**
EU Member States involved: **14**

Key words
Research Governance
Cybersecurity skills
Cybersecurity certification
Community engagement
International cooperation
Strategic Autonomy

Last updated 26 February 2019

More than **160 partners** from **26 EU Member States**

More info at:
https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

European Commission

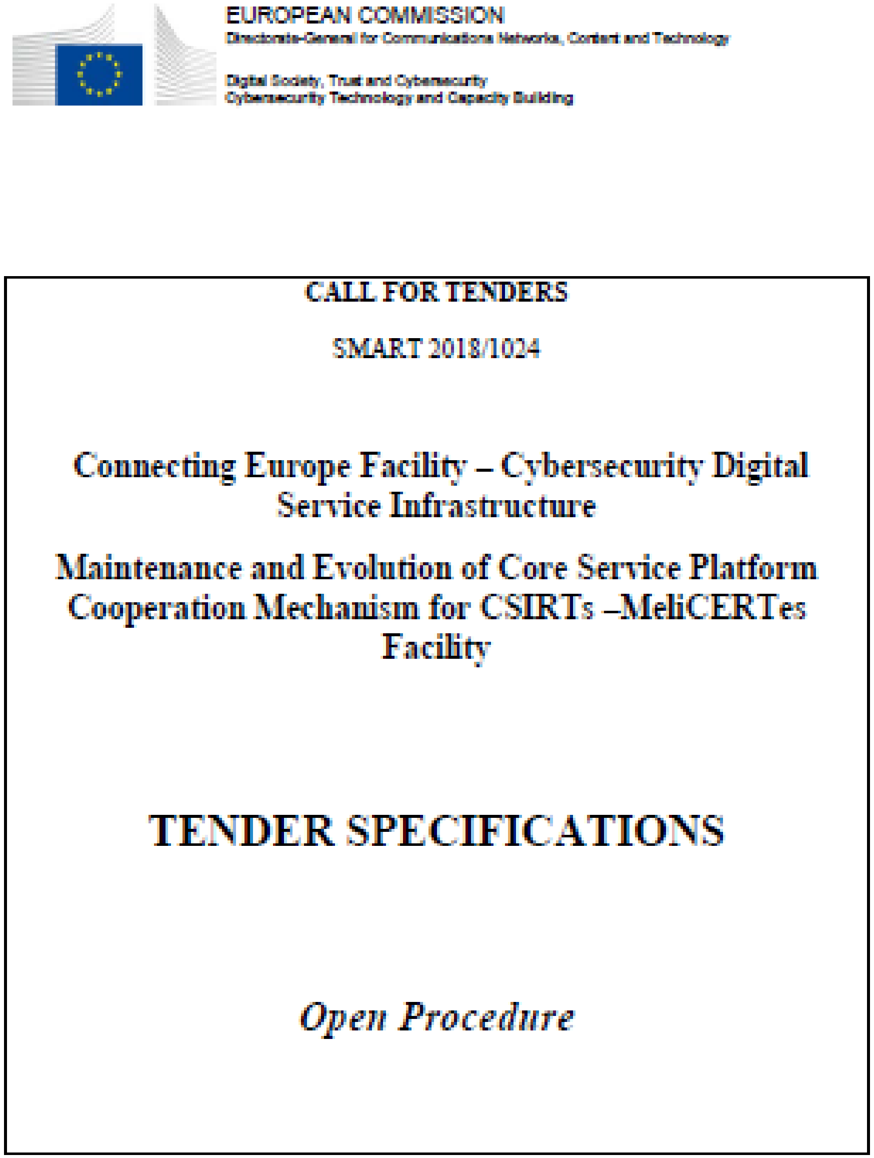
MeliCERTes

Information sharing platform for the Computer Security Incident Response Teams (CSIRTs)

MeliCERTes
Call for tenders

Further call info:

https://etendering.ted.europa.eu/cft/cft-display.html?cftId=4340



EUROPEAN COMMISSION
Directorate-General for Communications Networks, Content and Technology

Digital Society, Trust and Cybersecurity
Cybersecurity Technology and Capacity Building

CALL FOR TENDERS

SMART 2018/1024

Connecting Europe Facility – Cybersecurity Digital Service Infrastructure

Maintenance and Evolution of Core Service Platform Cooperation Mechanism for CSIRTs –MeliCERTes Facility

TENDER SPECIFICATIONS

Open Procedure

European
Commission

Thank you for your attention!