The Role of ENISA in the Implementation of the NIS Directive

Anna Sarri | Officer in NIS

CIP Workshop | Vienna | 19th September 2017

European Union Agency for Network and Information Security

Positioning ENISA activities

CAPACITY

- ✓ Hands on activities

POLICY

- ✓ Support MS & COM in Policy implementation
- ✓ Harmonisation across EU

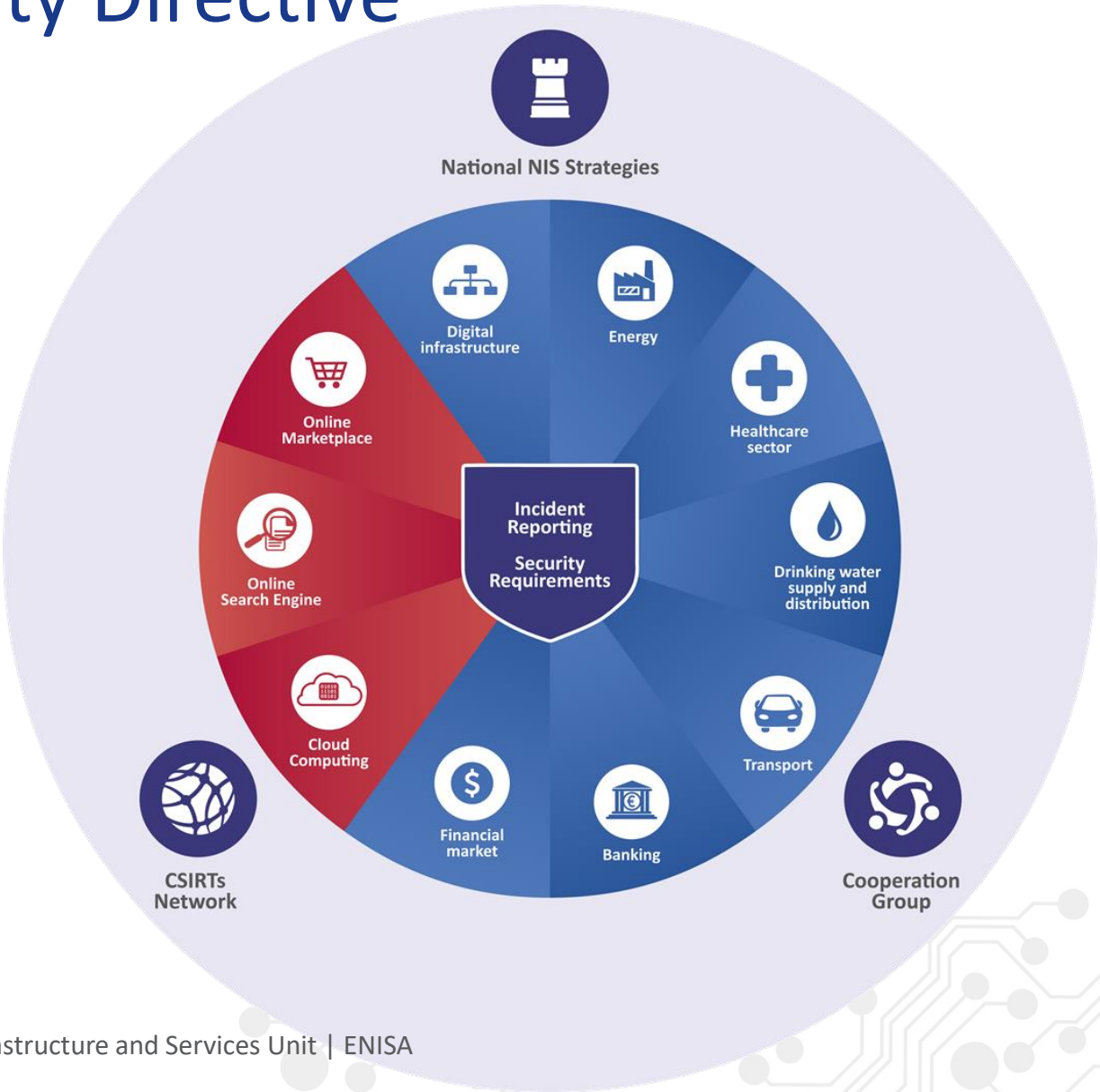
COMMUNITY

Mobilizing EU communities

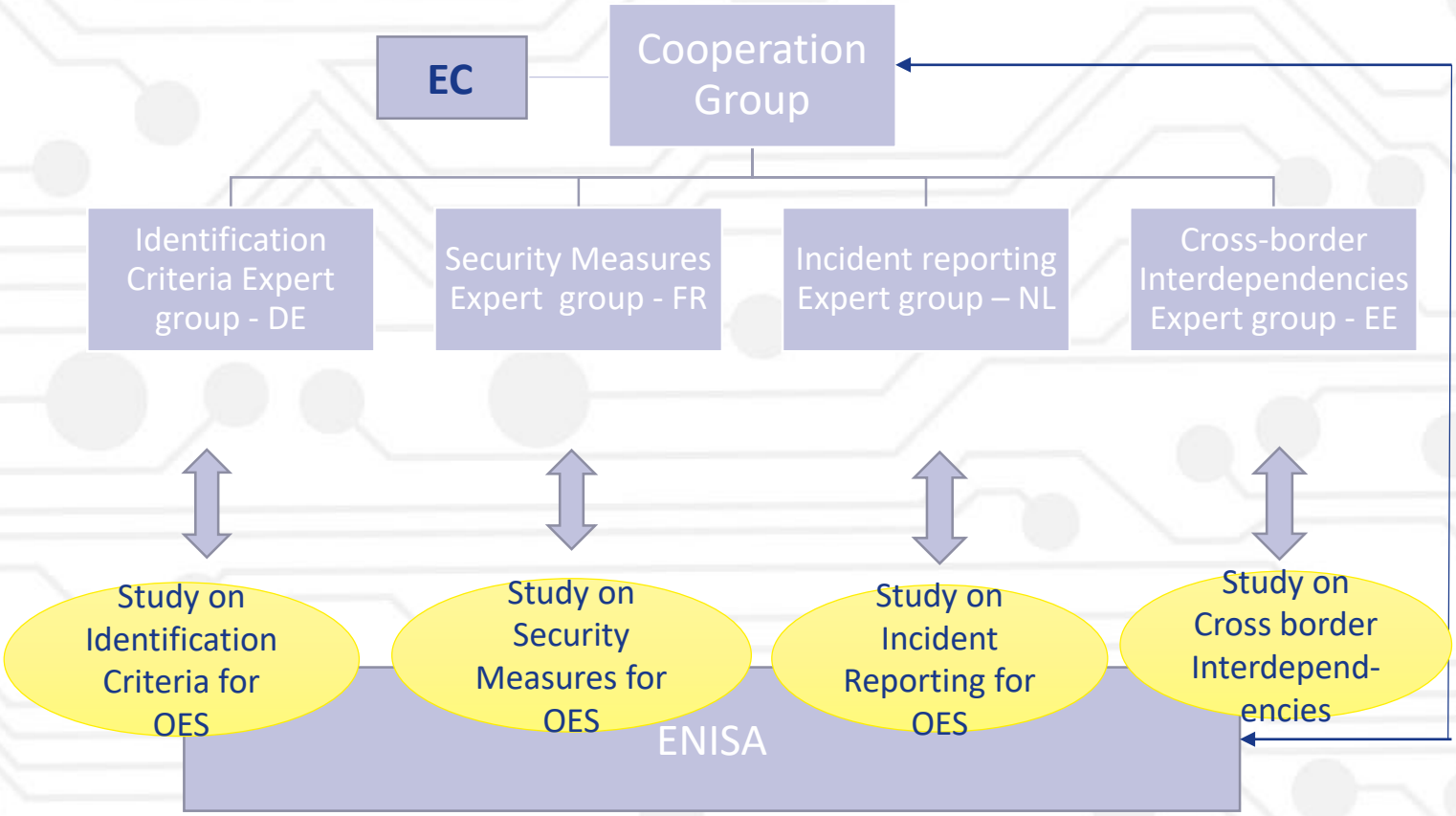
EXPERTISE

- ✓ Recommendations
- ✓ Independent Advice

The Network and Information Security Directive



Co-operation Group & ENISA



National Cyber Security Strategies

- All 28 MS have a NCSS
- Challenges:
  - Effective cooperation between public stakeholders
  - Establish trust between public and private stakeholders
  - Lack of resources
  - Lack of common approach and awareness for privacy
  - The implementation of vulnerability and risk analysis
- MS are considering reviewing their NCSS in the light of the NISD

ENISA Supports the Member States

ENISA NCSS
EU map

ENISA
REPORTS

E-Learning
&
Workshops

ENISA NCSS
Expert Group

Identification criteria for OES

Main steps for MS to create and list OES:

- **Identify the essential services** that are critical for societal and economic activities.
- **Identify operators of essential services:** define specific criteria and thresholds.
- **Identify critical business processes and assets that support the provision of essential services.**
- **Create a list of OES.**
- **Review and update the list of OES every two years.**

Key findings

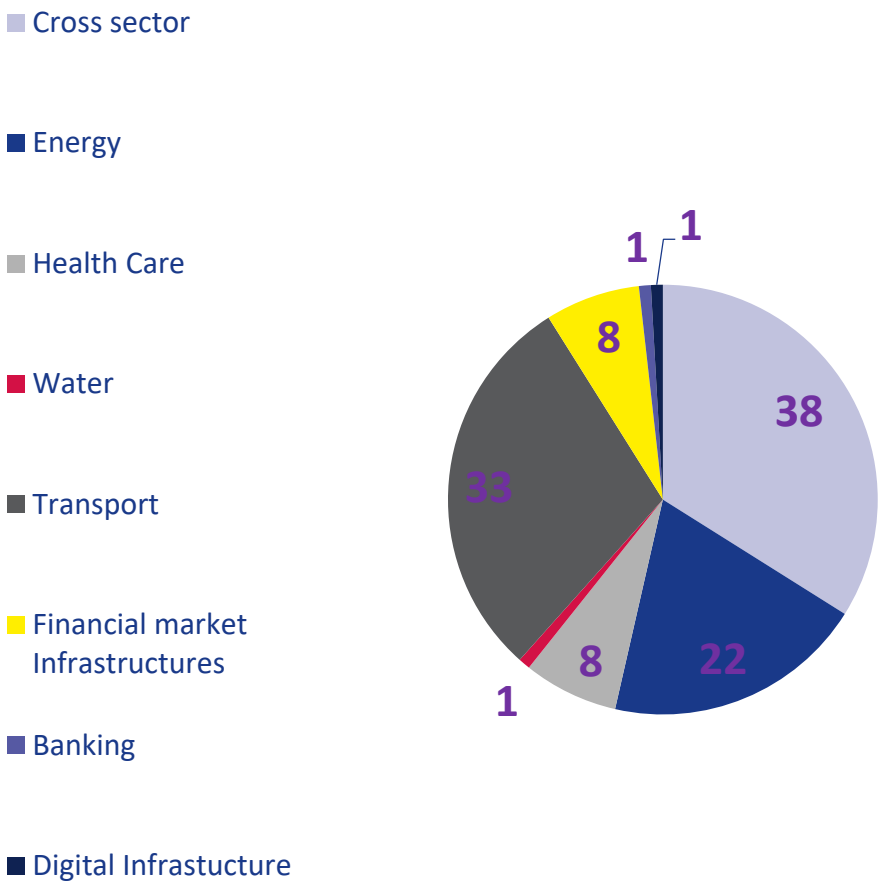
- For most MS, **the identification process of essential services and OES is in an initial phase.**
- Selected MS have **different registration approaches** for operators of essential services.
- Identified lists of essential services are characterised by **significantly different levels of description.**
- Most MS have developed methodologies to identify **Critical Infrastructures,** not services.
- The **number of identified operators** depend on the size of the country.

- The ***state-driven*** approach where the leading role is assumed by one or more governmental agencies/ministries that have the mandate to identify the Essential Services and OES - in most of the cases the responsible ministries.
- The ***operator-driven*** approach where operators self-assess if specific criteria are met and then register to the list of OES. This approach does not require the national authorities to identify individual operators of critical infrastructures – it is the operators' duty to notify the authorities when they fall under the predefined criteria.

Challenges

- Adaptation of existing methodologies to NIS Directive requirements.
- Difficulty in **matching the criteria** of the NIS directive to the criteria that have already been developed.
- Challenges in **threshold definition**. Sometimes they are not at all necessary for small countries where only one operator exists in a given sector.
- Cooperation with the **private sector**
- Challenges regarding NIS Directive **definitions**.

Security Measures for OES



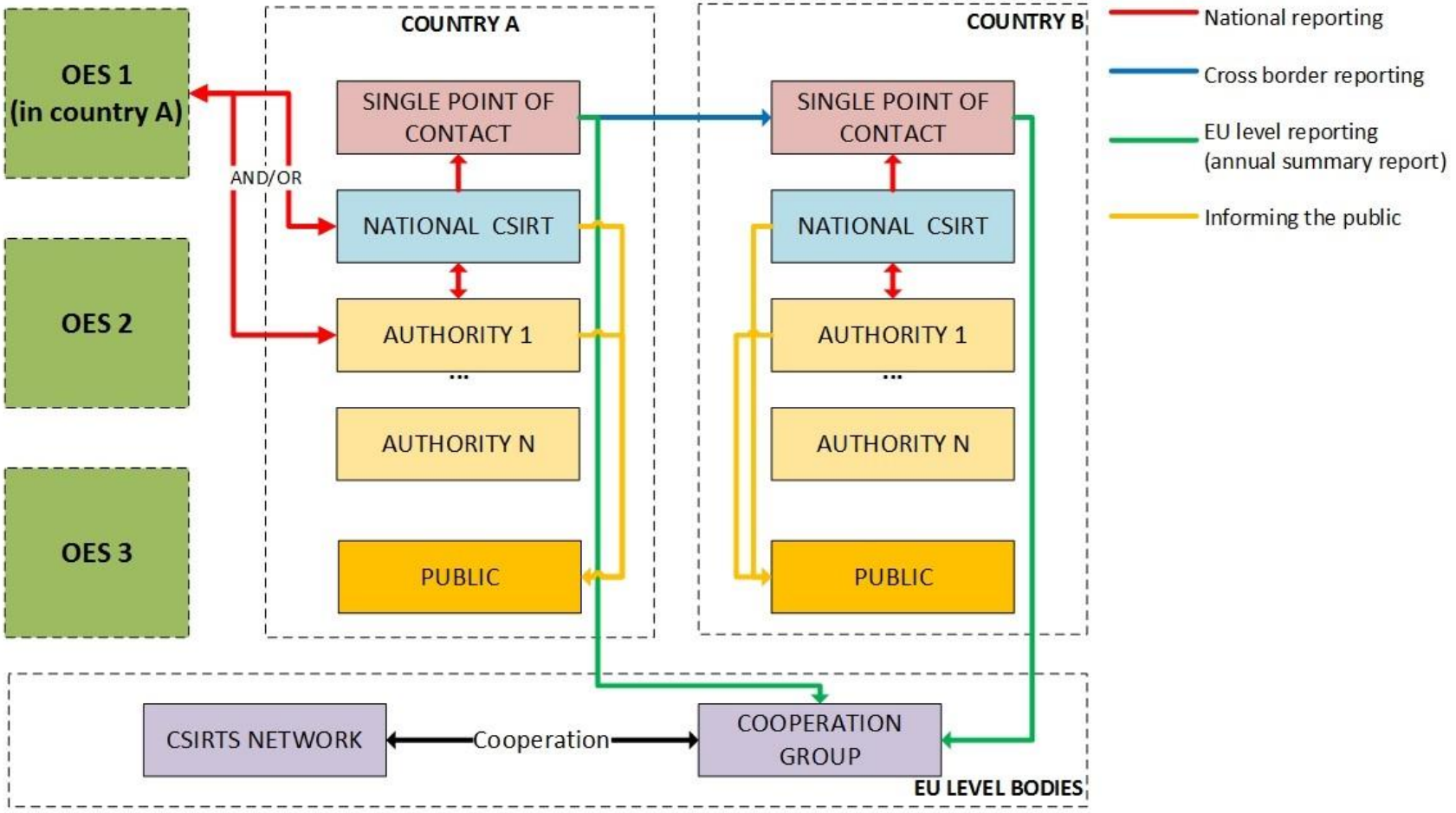
Desktop Research on:

- Security standards & good practices per NISD sector
- Country specific standards, good practices, laws & regulations
- Risk assessment & Risk Management methodologies
- 112 International standards & Good practices

Cooperation group work stream on Security Measures for OES

1. Information Security Governance & Risk Management
2. IT Reference Security Architecture & Management of third parties
3. Security Operations
4. Continuity of Operations
5. Logical and Physical Security
6. Computer Security Incident Management
7. Compliance and Reporting Framework
8. Systems Development and Acquisition

Incident Reporting for OES



Thank you

PO Box 1309, 710 01 Heraklion, Greece

Tel: +30 28 14 40 9710

info@enisa.europa.eu

www.enisa.europa.eu