

Enhancing the security of CIIPs in Europe - ENISA's Approach

Dimitra Liveri

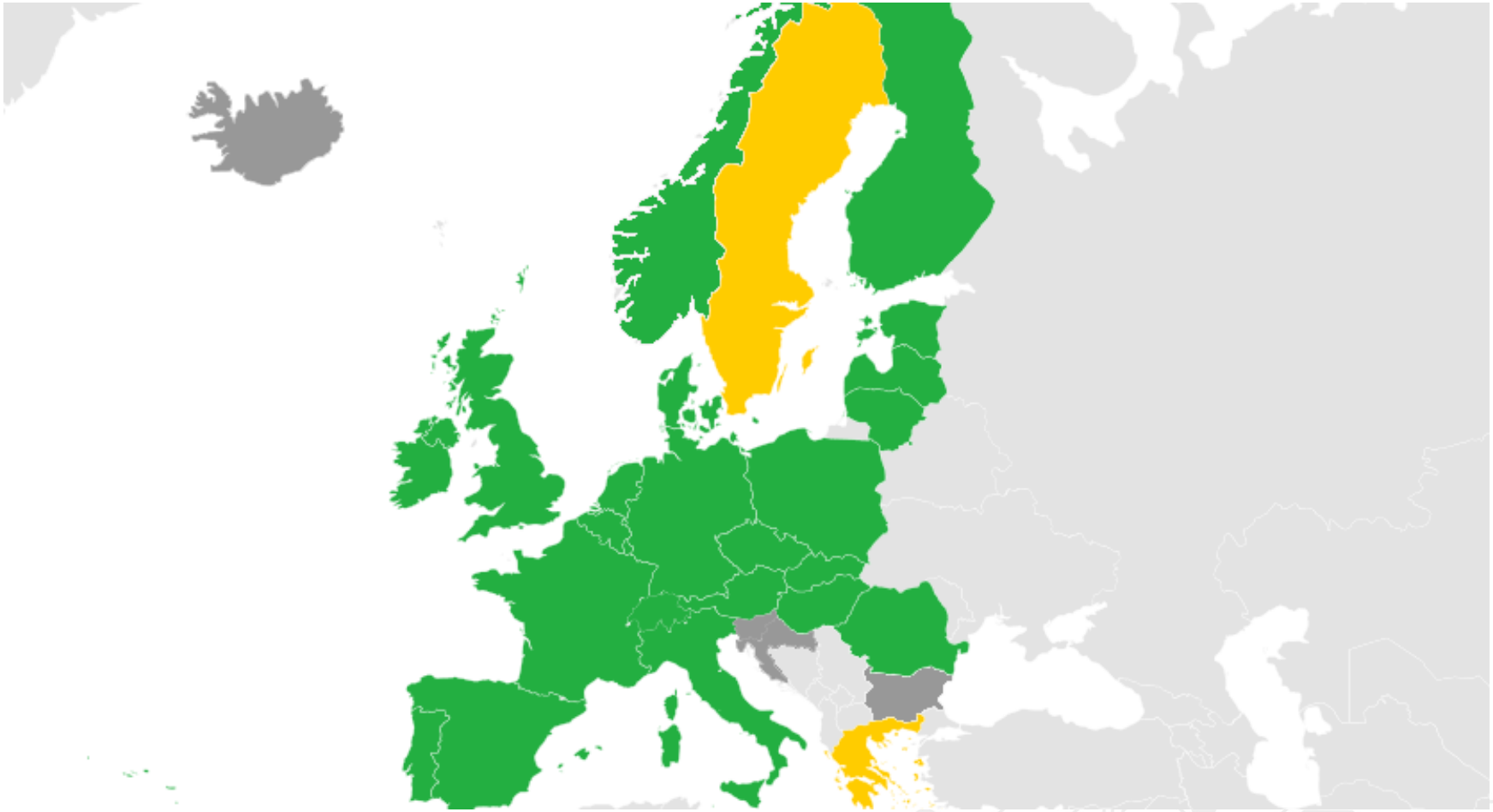
Network and Information Security Expert

European Union Agency For Network And Information Security

Securing Europe's Information Society

Positioning ENISA activities

National Cyber Security Strategies in EU



Critical Information Infrastructure (CII)

“ ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.) ”

Critical Sectors in EU MS

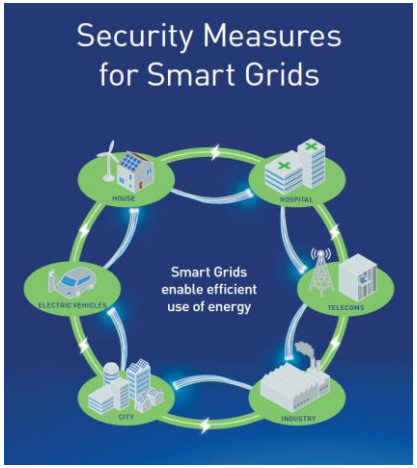
Sectors	Energy	ICT	Water	Food	Health	Financial	Public & Legal Order	Civil Admin.	Transport	Chemical & Nuclear Industry	Space & Research
AU	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
BE	✓	✓				✓			✓		
CZ	✓	✓	✓	✓		✓		✓	✓		
DK	✓	✓		✓	✓				✓		
EE	✓	✓	✓	✓	✓	✓	✓	✓	✓		
FI	✓	✓	✓	✓	✓	✓	✓		✓		
FR	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
DE	✓	✓	✓	✓	✓	✓	✓		✓		
EL	✓								✓		
HU	✓	✓	✓	✓	✓	✓	✓		✓		
IT	✓								✓		
MT	✓	✓			✓	✓		✓	✓		
NL	✓	✓	✓	✓		✓	✓	✓	✓	✓	
PL	✓	✓	✓	✓	✓	✓		✓	✓	✓	
SK	✓	✓	✓		✓				✓		
ES	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓
UK	✓	✓	✓	✓	✓	✓		✓	✓		
CH	✓	✓	✓	✓	✓	✓		✓	✓		

Critical Information Infrastructure Protection in Europe: ENISA efforts

Communication networks: Critical information Infrastructure and Internet Infrastructure

ICS SCADA

Smart grids



eHealth

Finance

Transport

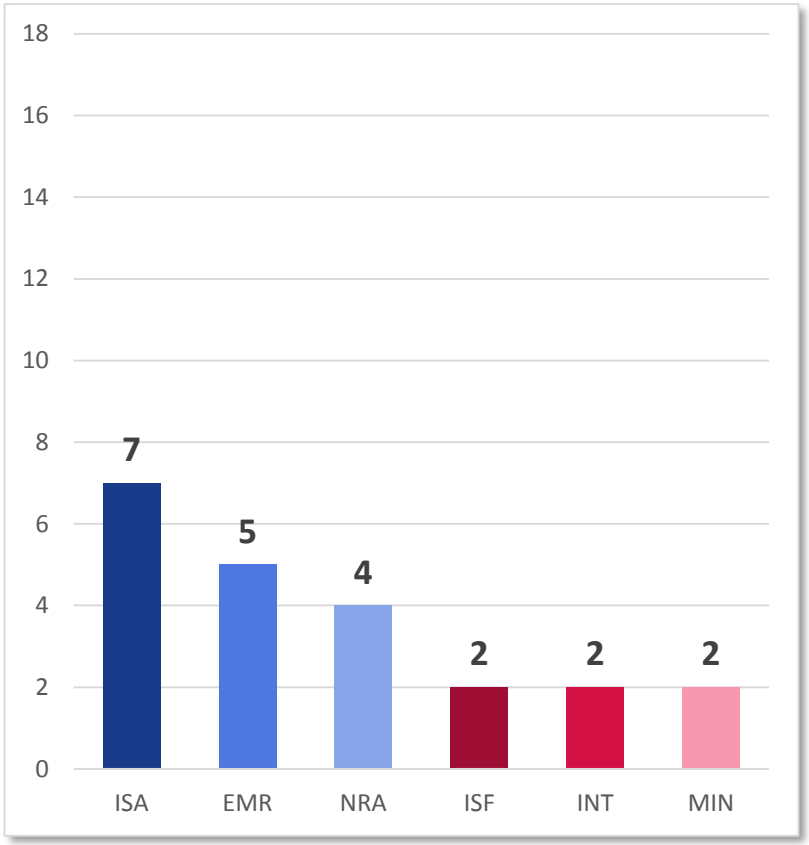
2015 studies on CIIs

- Stock Taking, Analysis and Recommendations on the protection of CIIs
- Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors
- Communication networks dependencies in smart grids
- Security and resilience for E-health infrastructure
- Security and resilience for cloud computing in the Finance sector

Key Findings

Key Findings

National Authorities

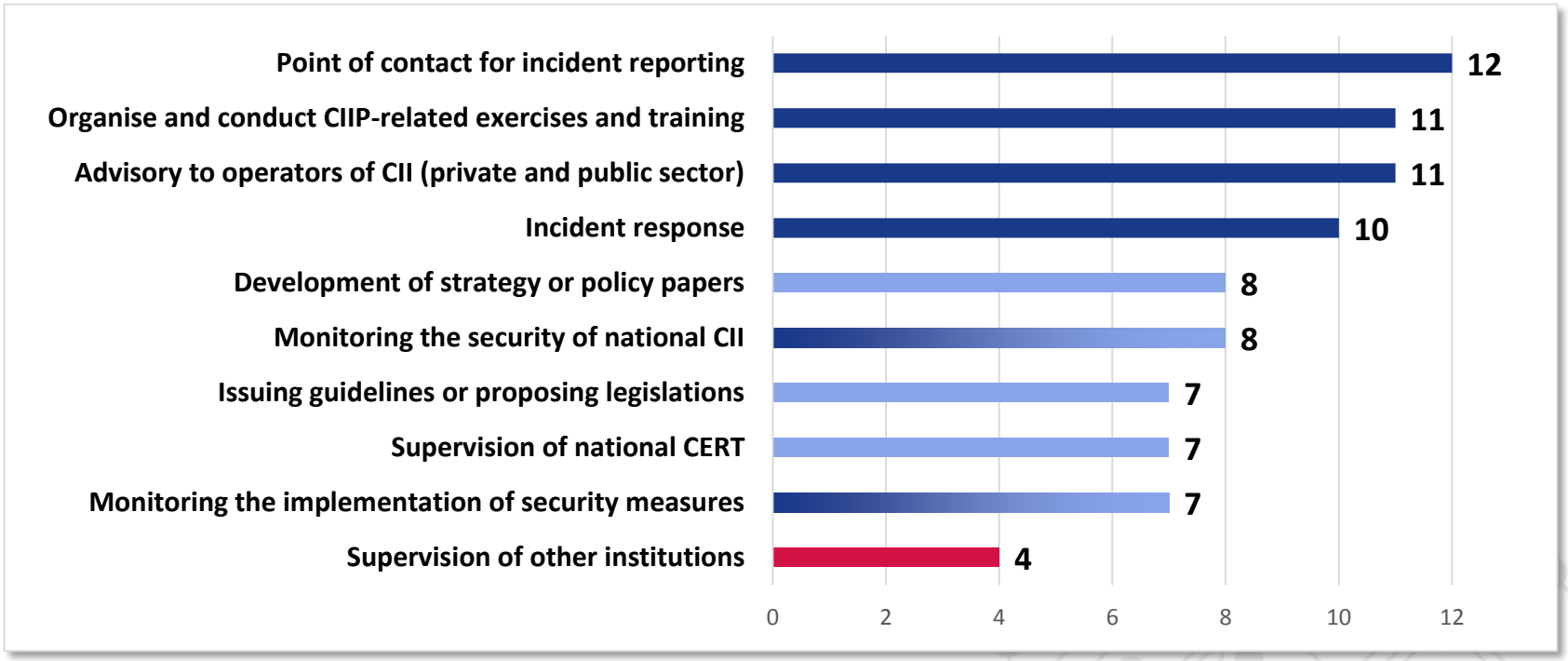


- Most countries have assigned responsibility to Information security agencies, Emergency or CIP agencies, or National regulatory agencies
- Reason: Historical development or indicator for how the problem is perceived
- Only four countries have assigned CIIP to Information security forums or Intelligence security agencies
- In two cases, responsibility is shared between a Ministry and a public agency

Key Findings

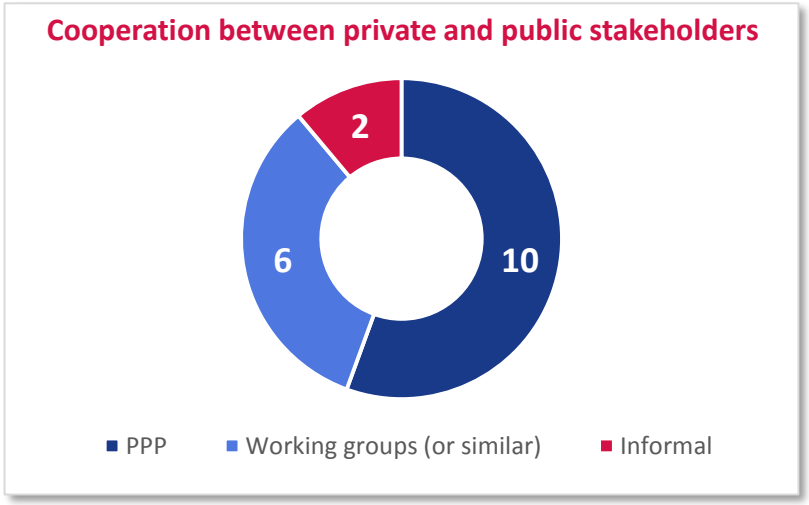
Task and Responsibilities

- Most tasks are on the operational level (10-12 / out of 12 examined countries) (darkblue)
- 7 to 8 countries have been assigned responsibilities on the politico-strategic level (lightblue)
- 4 countries have been tasked with the supervision of institutions other than CERT. These include mainly regulatory tasks (red)

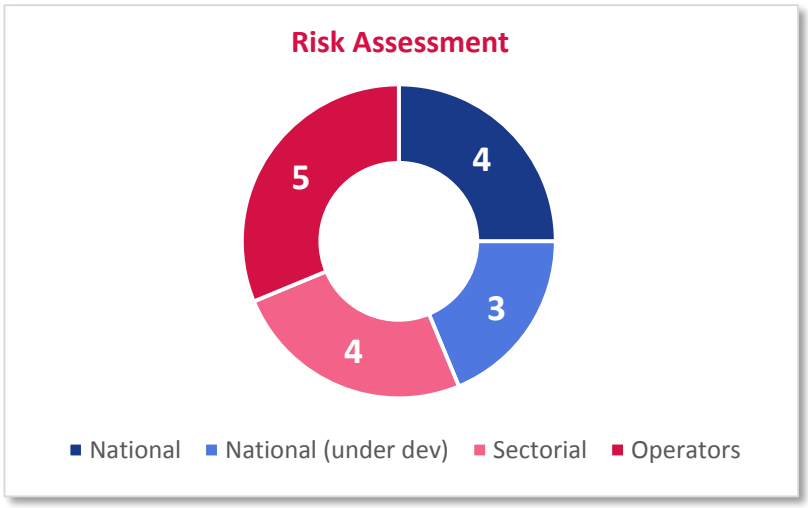


Key Findings

Public-private Cooperation | Risk Assessment



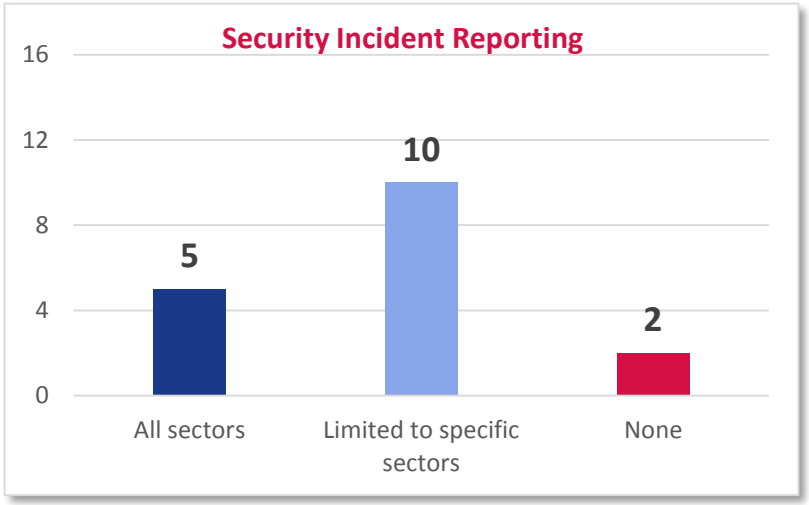
- Ten out of 18 examined countries have developed partnerships with private actors
- Trend towards more institutionalised forms of cooperation with the private stakeholders



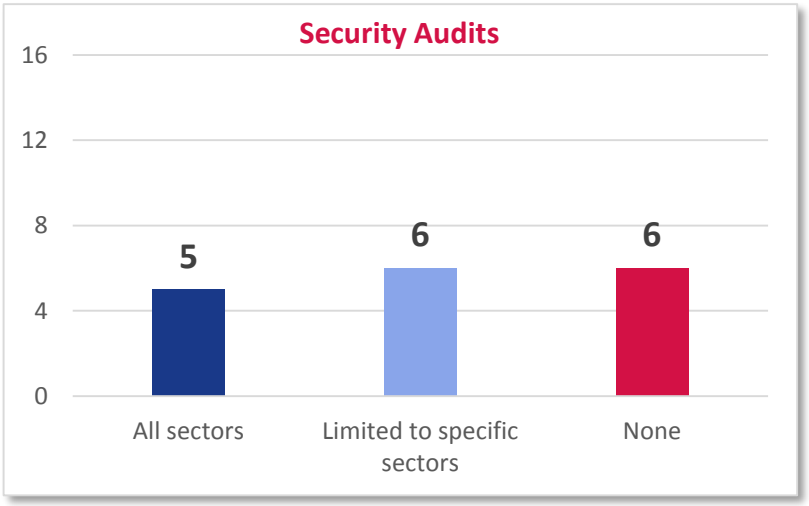
- The majority of the 16 examined countries has conducted RA on a national level or a planning to do so
- This can be seen as an indicator for how a government perceives the problem

Key Findings

Obligations and Requirements



- Only five of 17 examined countries have established mandatory incident reporting across all sectors
- All Member States have implemented mandatory incident reporting in the telecommunications sector
- Other important sectors: Finance, Energy, Public Administration



- Six countries have implemented no mandatory security audits in any sector
- Security Audits are either of less priority for countries or hard to implement

Governance of CIIP

Governance of CIIP

Three profiles of CIIP-governance have been examined

- Centralised approach
- Decentralised approach
- Co-regulation with private sector

- The different profiles illustrate specific forms of CIIP governance, which are defined by their shared characteristics. The profiles are not exclusive types, but are rather points on a spectrum
- These profiles can help to understand how CIIP is organised in the individual Member States
- Can help to understand and what CIIP-measures and -actions can possibly be transferred from one Member State to another

Governance of CIIP

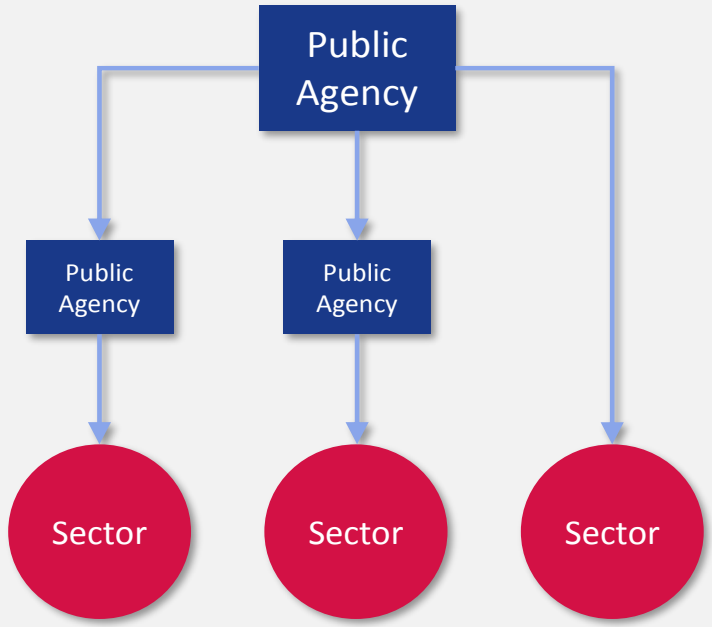
The centralised approach

The centralised approach is characterised by

- Central authority across sectors
- Comprehensive legislation

Examples

- France



Governance of CIIP

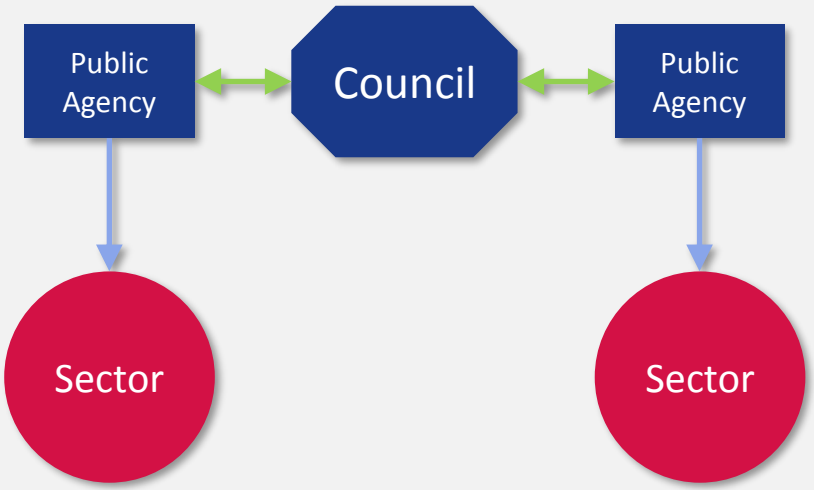
The decentralised approach

The decentralised approach is characterised by

- Principle of subsidiarity
- Strong cooperation between public agencies
- Sector-specific legislation

Examples

- Sweden



Governance of CIIP

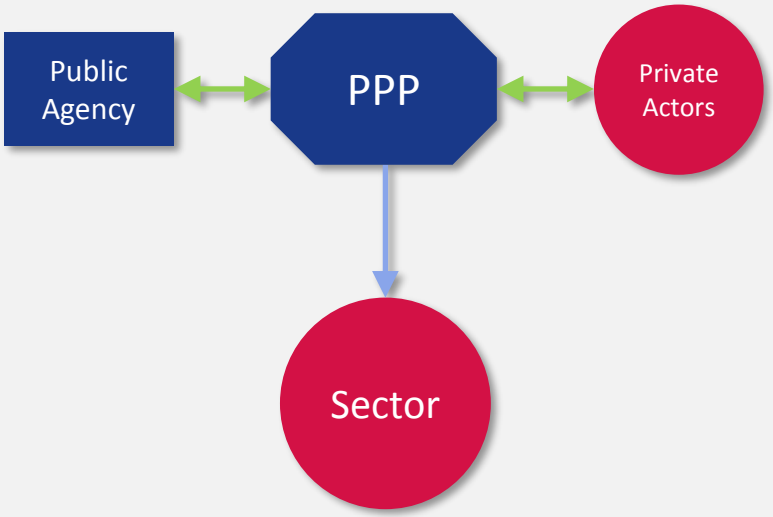
The co-regulation approach

The co-regulation approach is characterised by

- Institutionalised cooperation with the private sector
- Horizontal relationship between public and private parties

Examples

- Netherlands



Goals

01 Raise the level of awareness on CIIP in Europe

02 Support Private and Public Sector with focused studies and tools

03 Facilitate information exchange and collaboration

04 Foster the growth of communication networks and industry

05 Enable higher level of security for Europe's Critical Infrastructures

Thank you

Dimitra Liveri

resilience@enisa.europa.eu

https://www.enisa.europa.eu/scada