



# Cyber Security in Europe



## ENISA supporting the National Cyber Security Strategies – An evaluation framework

Liveri Dimitra

Security and Resilience of Communication Networks Officer



[www.enisa.europa.eu](http://www.enisa.europa.eu)

# Securing Europe's Information Society



# ENISA Activities

Recommendations

Policy  
Implementation



Hands on



**CERT Exercises Handbook**  
Document for teachers  
Deliverable – 2012-11-26




# EU Cyber Security Strategy





## Five Strategic Objectives

- Achieving cyber resilience
- **Drastically reducing cybercrime**
- Developing cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- **Developing the industrial and technological resources for cybersecurity**
- Establishing a coherent international cyberspace policy for the European Union and promote core EU values.

 ENISA explicitly called upon.



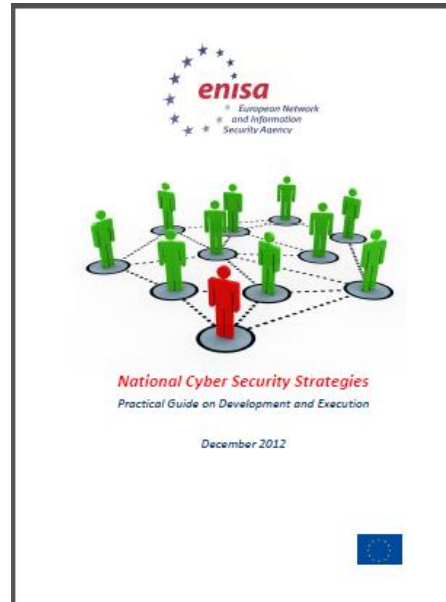
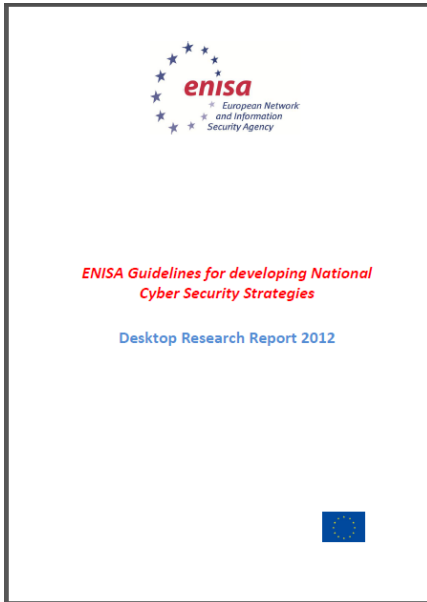


# National Cyber Security Strategy Context

- Protection of citizens, business and government
- Raising awareness on cyber security issues (citizens, business)
- Enhancing cyber security and critical information infrastructures protection (health, finance, transport, energy sector) in national level.
- Trusted information sharing and cooperation (effective PPPs)



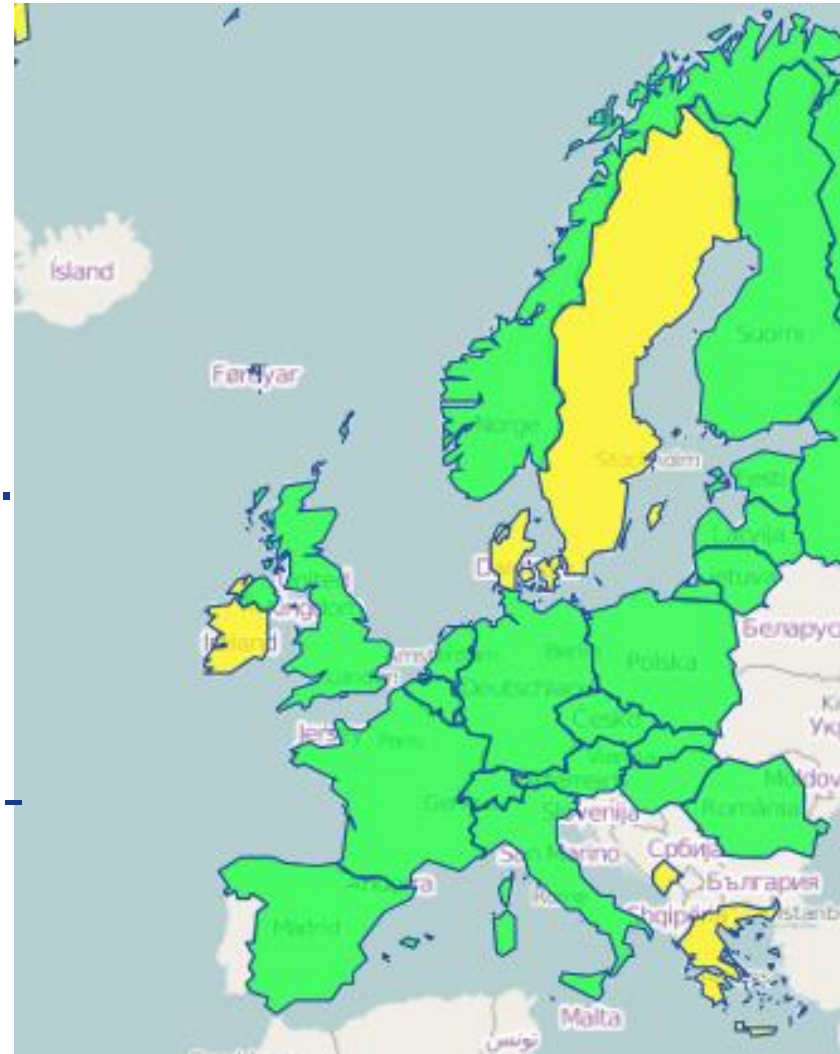
# ENISA work in supporting NCSS



- 2012: Desk research on cyber security strategies in the EU
- 2012: Good practice guide on how to design and implement cyber security strategies
- 2013: Inventory of NCSS in EU

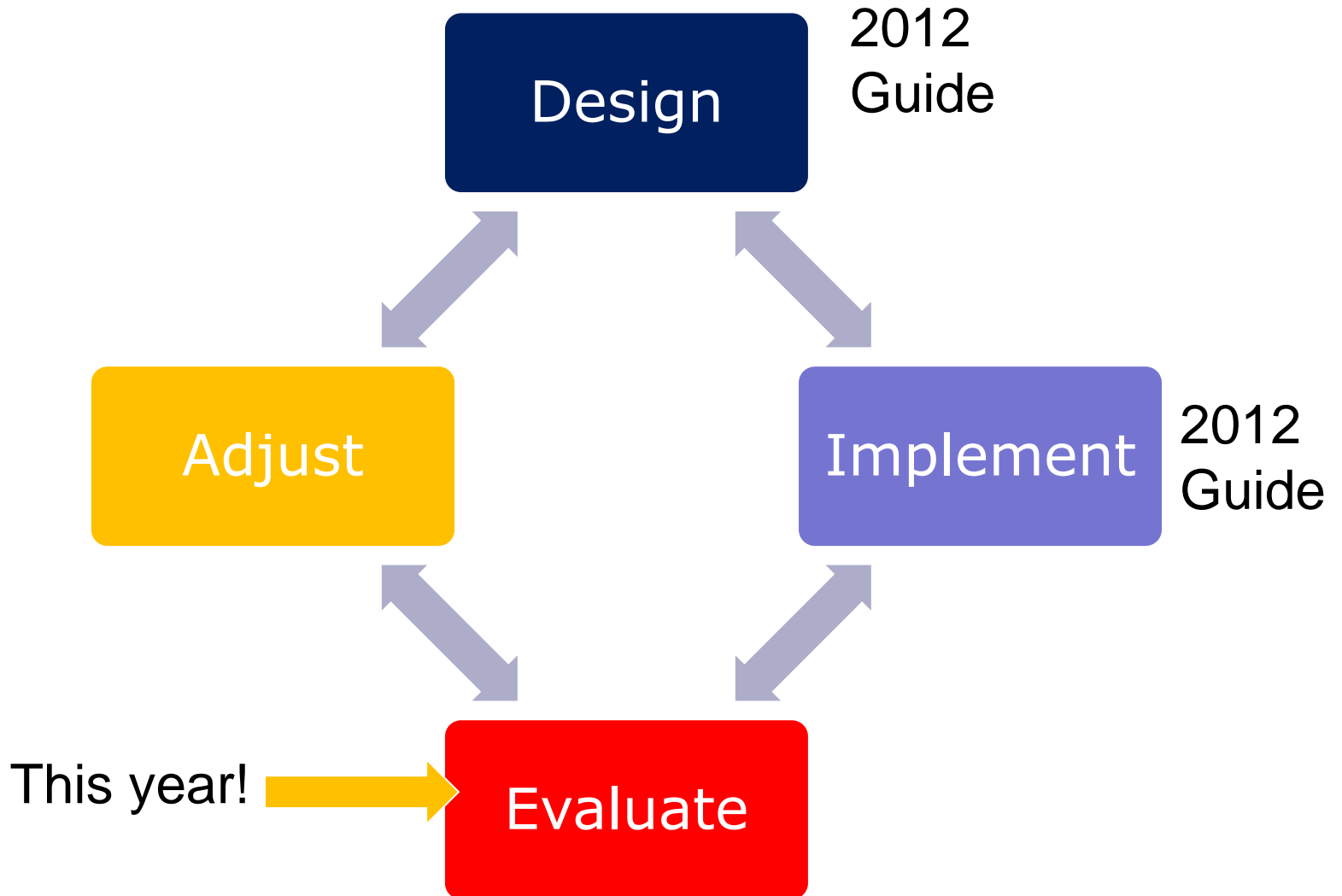
# National Cyber Security Strategies in the EU

- Source:  
<http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>

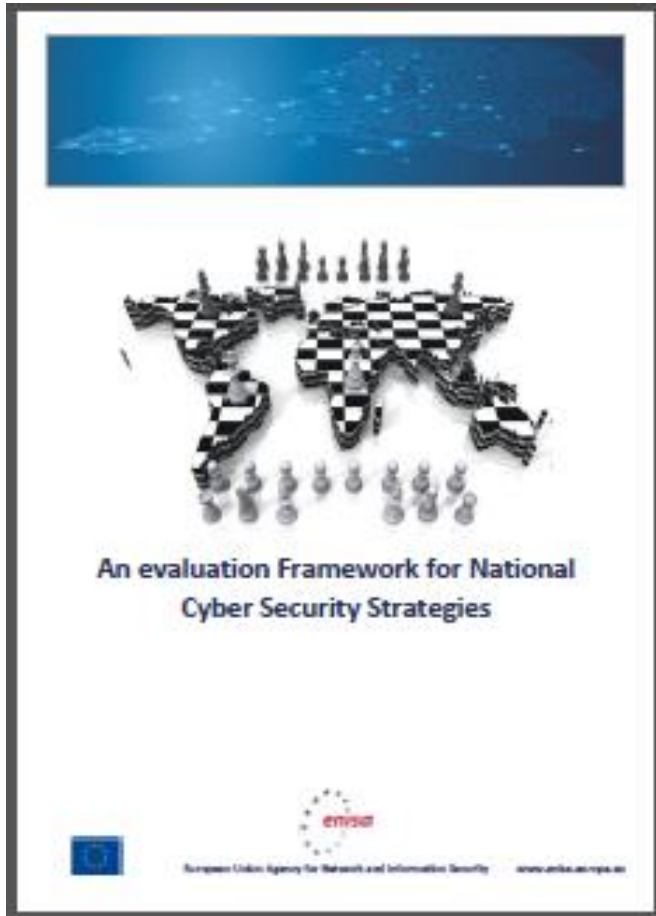




# ENISA doctrine: NCSS Lifecycle



# Evaluation framework for NCSS



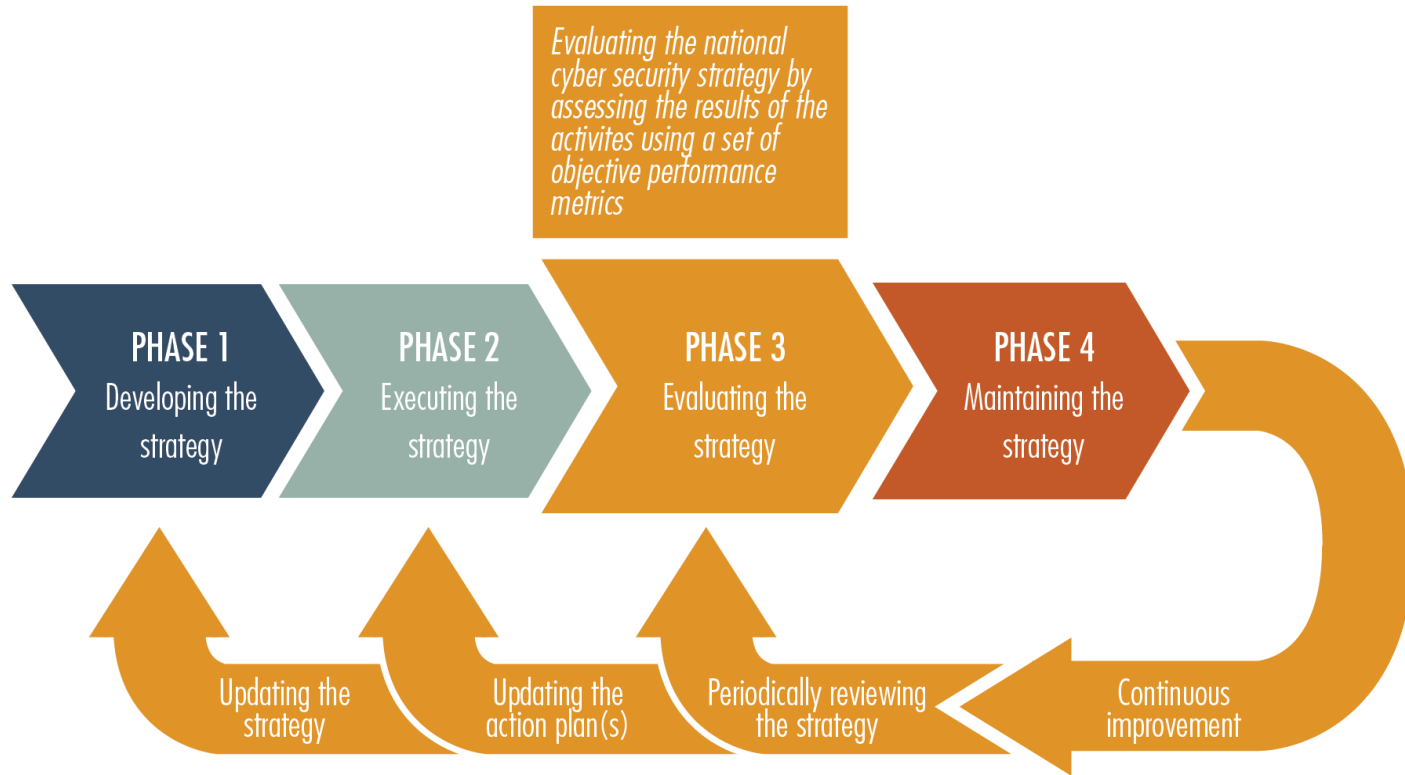
- Evaluation framework for NCSS
- Objectives of the evaluation
- Logic model and steps to follow (inputs and outputs)
- Key performance indicator per objective



# Why evaluate?

- Allow learning from past experience and make the according adjustments
- Evaluation procedure can offer credibility and enhance trustworthiness of the scheme
- Evidence of effectiveness of the plan and of involvement of the stakeholders
- Catalyses discussion with stakeholders
- CHALLENGE: Correct evaluation need investment in time, resources and money

# Evaluation in the Lifecycle

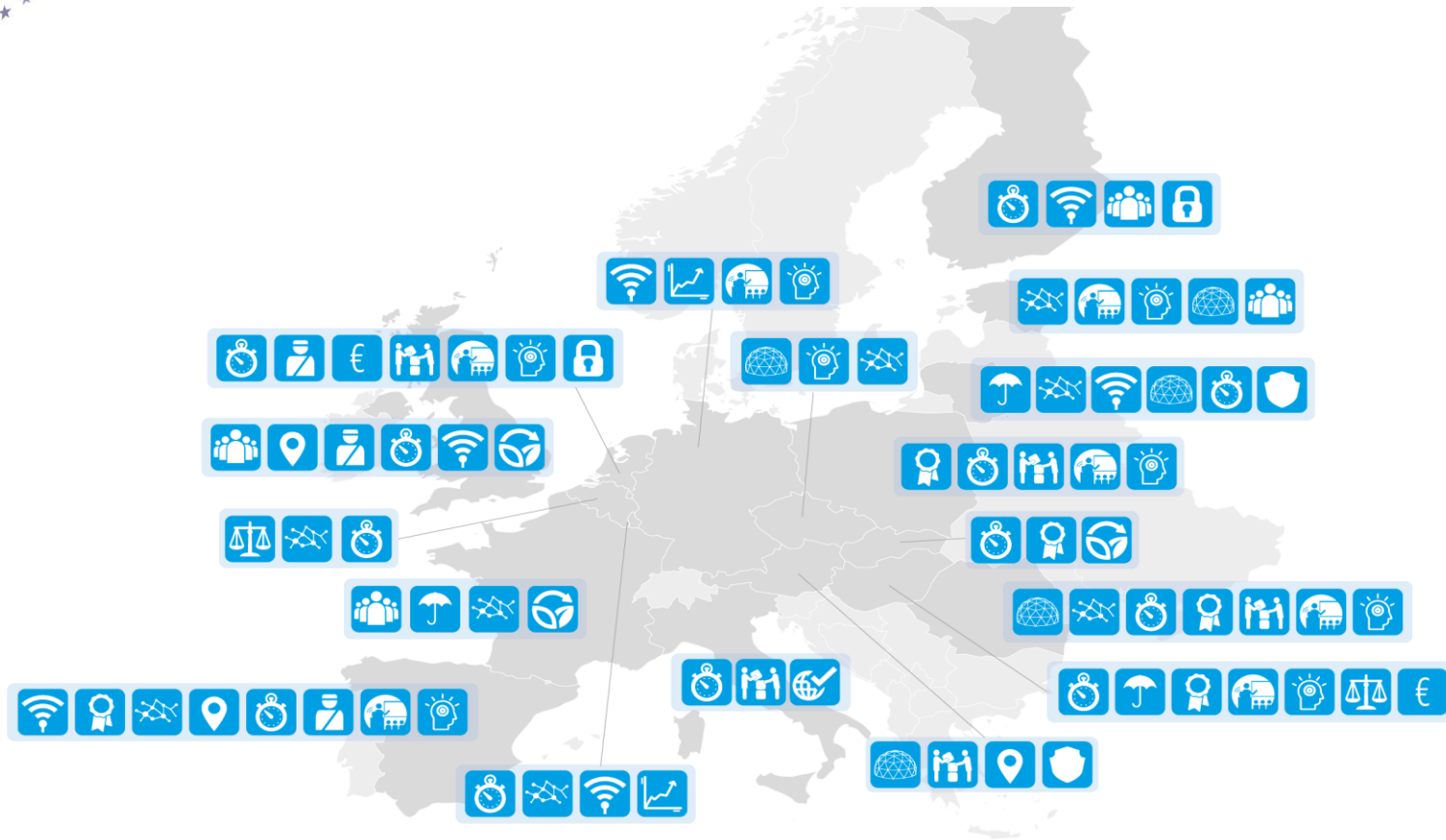








# What do we want to achieve?

- Establish and implement legislation
- Preparedness, resilience and adequate response to cyber-threats and attacks
- Protect critical information infrastructures
- Tackle cyber crime
- Raise awareness
- Train and educate
- Promote economy reliant on digitalised industry
- Secure cyber space
- Invest on ICT and innovation in security and privacy
- Ensure quality of IT and communication products through security standards

# High level goals



-  Establish and implement legislative framework
-  Citizens' perception of sufficient data protection
-  Preparedness, resilience and adequate response to cyberthreats and attacks
-  Safe use of information and communication in the cyberdomain by citizens, businesses and authorities

-  Establish and clarify roles in collaboration between the public and private sector
-  Protect digital national information resources
-  Promote economy reliant on digitalized industry
-  Secure safe place to do business

-  Invest in ICT and innovation for cybersecurity and privacy
-  Education and training
-  Awareness raising
-  Quality of IT and communication products and security standards

-  Protection and efficient functioning of critical information infrastructure
-  International leadership position
-  Tackle cybercrime
-  Secure cyberspace with respect for fundamental rights and values

-  Sustainability: shape an open, stable and secure cyberspace
-  Secure vital national functions and interests against cyber threats and attacks
-  Endorse and respect certain rules of behaviours in the digital arena consistent with national values





## How will we achieve it?

- Develop legislation and standards
- Establish public private partnerships
- Enhance international cooperation
- Create a culture of information security: inform, educate, raise awareness
- Invest in research, development and innovation
- Build competence capabilities on relevant actors

# Specific Objectives



- 

Develop standards and norms, legislation
- 

International cooperation
- 

Create a culture of security: inform, educate, raise awareness
- 

Security of services delivered in cyberspace
- 

Counter national and international criminal activities
- 

Strategic collaboration between authorities, business and academics
- 

Protect critical information infrastructures
- 

Research, development and innovation
- 

Competence and capabilities building of involved actors
- 

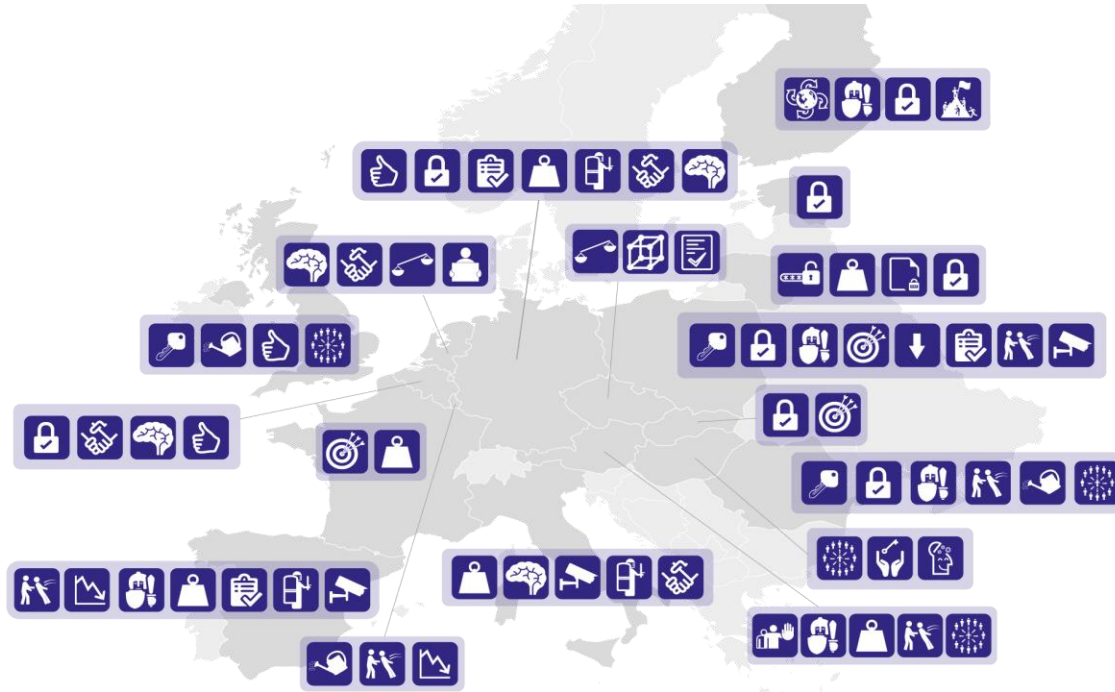
Threats tracking, risk assessment and response



# Long term impact

- Critical information Infrastructure and services protection:
  - Better coordination and greater competence between actors
  - Elimination of disruptions
  - Strengthening capabilities
- Business and Innovation
  - Societal development
  - Effective and innovative ebusiness solutions
  - Expanding digital economy
- Rights and Society
  - Protection of personal data and privacy
- General
  - Secure, credible and reliable cyber space

# Long term impact



**(Critical) information infrastructure and services: information security**

- Better coordination and greater competence of public and private actors involved in the information infrastructure security
- Ensure confidentiality, integrity and accessibility of electronic information and services
- Reduction or elimination of disruptions in the normal functioning of essential services that are vital to functioning of society
- Strengthened capabilities protecting critical information infrastructures, communication networks and services

**Business & innovation**

- A cyberspace optimal for societal development
- Creation of an internationally recognized competitive and exportable cybersecurity cluster
- Development of effective and innovative ebusiness solutions
- Establishing a cost-effective structure avoiding excessive burden on private entities
- Foster a growing business sector and expanding digital economy
- Innovative public services
- Maintaining and promoting economic and social prosperity
- Stimulate technological capabilities and national academic initiatives in security and privacy knowledge

**Rights and society**

- A balance between privacy, fundamental rights and liberties, free access to information with the need to guarantee security
- Protection of personal data and privacy
- Ability to counter online criminal activities
- Awareness and a culture of security among citizens and institutions

**Public – private relations**

- Allow citizens and businesses to safely handle their affairs with the government

**General**

- A cybersecurity policy consistent for all the involved agents
- A secure, credible and reliable cyberspace for all users
- Enhanced national security
- Greater confidence in safety of using cyberspace by citizens, businesses, public sector
- Increased resilience against cyberthreats and attacks
- International cooperation
- International leadership position
- Lower effectiveness of internet terrorism and lower costs of countering cyberterrorism
- Prevention of threats
- Better cybersecurity practices and procedures



## Usual approaches on evaluation

- Regular progress reports
- Security Committee assessment of the implementation and progress of specified objectives;
- Participating institutions provide an update;
- Promote the use of questionnaires among stakeholders to understand the training needs;
- Regular evaluation of security policies;
- Specific measures to evaluate the effectiveness of projects;
- Testing the efficiency of processes designed to deal with security risks.

# Examples of evaluation processes



Regular progress reports



Cyber Security Council or Security Committee assesses the implementation and progress of specified objectives



Enhance and evaluate education and on the job training programmes



Not mentioned



Participating institutions provide a status update



Presidency of the Council of Ministers drafts a text on the activities in relation to cyberspace protection Annexed to the Annual Report to the Parliament on national security strategy and policies



Promote the use of questionnaires among stakeholders to understand their training needs



Regular evaluation of security policies



Regular review



Specific measures to evaluate the effectiveness of projects

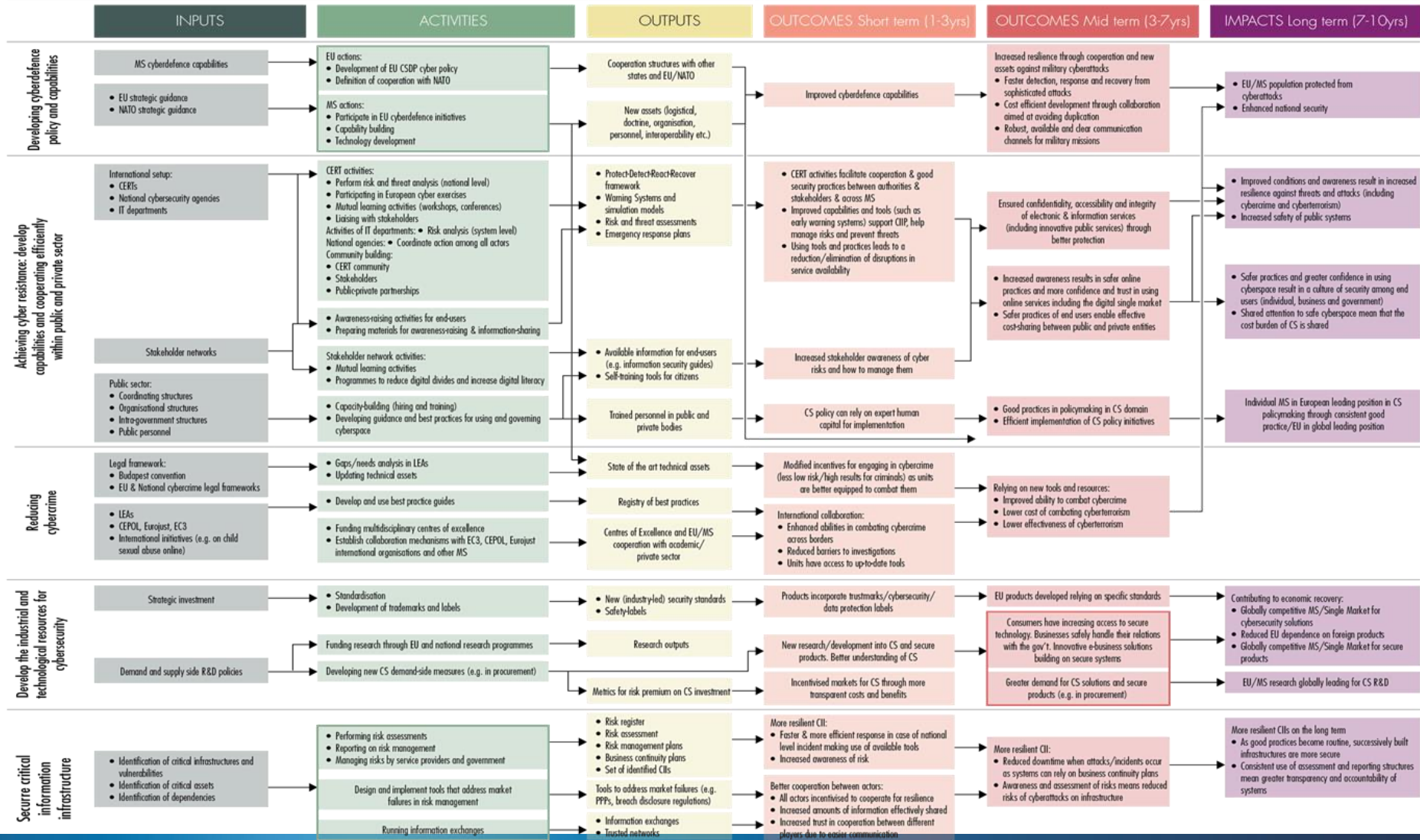


Testing the efficiency of processes designed to deal with security risks



# Logic model for evaluation

## LOGIC MODEL ELEMENTS FOR NCSS





# Key performance indicators

- Categorised by objective:
  - Cyber defence policy and capabilities
  - Achieving cyber resilience: developing capabilities and cooperating efficiently within public and private sector
  - Reducing cyber crime
  - Develop the industrial and technological resources for cybersecurity
  - Secure critical information infrastructure

## Example:

Key Performance Indicator	Evidence (what we should measure)
Setup of CERTs and/or National Security Agencies	Existence and mandate of the institutional actors (mission scope, agencies/ bodies mandate)
Existence or setup of public private partnerships on cyber security	Identification and structure of those partnerships, bodies involved and their role, activity reports
Identified risk and threats landscape	Risk analysis, threat analysis (conducted by CERTs or National Security Agencies)
Existence of organised national cyber security exercises	Activity reports
Enhanced capabilities: organised trainings for the public and private sector, mutual learning activities (workshops and conference).	Activity reports, event title, companies/stakeholders participated
Awareness raising activities for end-users (material, campaigns, events)	Material disseminated, campaigns/event organised, survey on citizens perception
Existence of developed response capabilities (react-recovery plans, early warning systems etc)	protect-detect-react-recover plan, early warning systems and simulation models, activity report



# ENISA Supporting the EU Strategies

- ENISA CERT community, trainings, recommendations and good practices on how to setup and run a national CERT
- Cyber Exercises, trainings on how to organize and run a national cyber exercise; pan European exercises
- Critical information infrastructures protection: security recommendations on ICS SCADA, Smart Grids, Telecom sector, Finance Sector (soon to introduce Transport and Health)
- Support public sector: Article 13a, Article 4
- Educating the citizens: October the Cyber Security Month
- Annual threat landscape: security on emerging technologies
- Enhancing privacy issues





# Outlook

- Cyber Security is important for the well functioning of the society and economy
- Critical Services and Infrastructures should be better protected from cyber attacks and threats
- MS recognize the importance and develop NCSS
- ENISA develops good practices for EU MS and Private Sector to address the emerging issues
- Sharing experiences and deploying good practices improves the situation quickly
- When it is necessary, additional regulatory measures are introduced to resolve issues
- Exercises are the guarantees that these protective measures work





# Thank you for your attention

Dimitra Liveri: [Dimitra.liveri@enisa.europa.eu](mailto:Dimitra.liveri@enisa.europa.eu)

For more information visit: <http://www.enisa.europa.eu>

Follow ENISA:       

