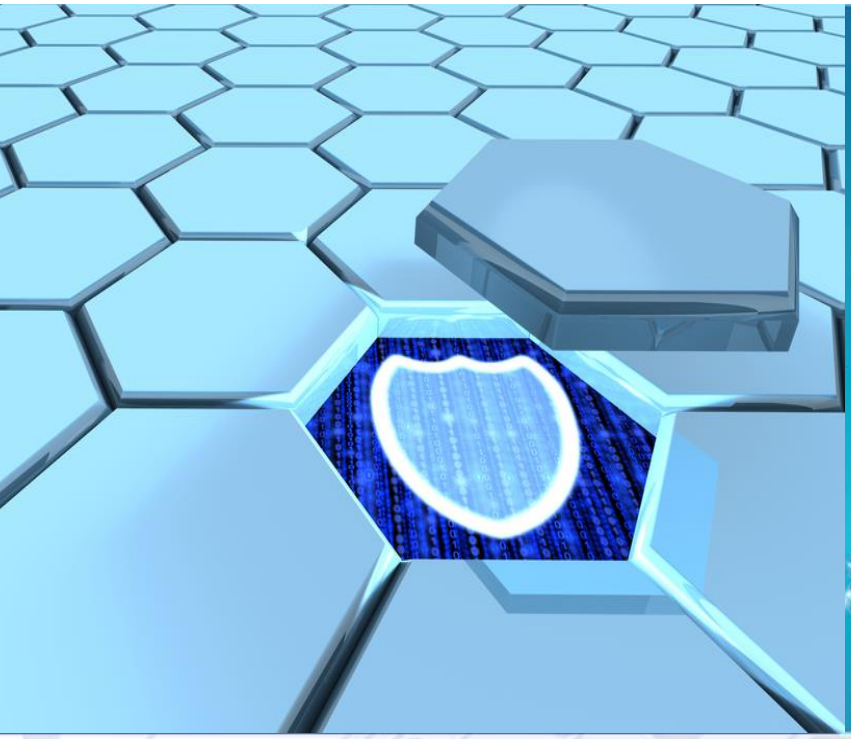

# NCSS Good Practice Guide

## Designing and Implementing National Cyber Security Strategies

NOVEMBER 2016

www.enisa.europa.eu European Union Agency For Network And Information Security

# About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

## Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquires about this paper, please use press@enisa.europa.eu.

## Acknowledgements

Special thanks to the NCSS experts group (https://resilience.enisa.europa.eu/enisas-ncss-project), and the representatives from the Member States for their contribution to this study.



ISBN: 978-92-9204-179-3 DOI: 10.2824/48036

# Table of Contents

# Executive Summary

To meet current and emerging cyber security threats, EU Member States need to constantly develop and adapt their cyber security strategies. National cyber security strategies (NCSS) are the main documents of nation states to set strategic principles, guidelines, and objectives and in some cases specific measures in order to mitigate risk associated with cyber security. Following a high-level top-down approach, NCSS set the strategic direction for subsequent actions.

Moreover, the recently adopted NIS Directive requires EU Member States to develop and adopt a national cyber security strategy (NCSS). If needed, Member States can call upon ENISA to assists them in drafting a NCSS. Within three months after the adoption of their NCSS, EU Member States need to forward the strategy to the European Commission.

ENISA published its first National Cyber Security Strategy Good Practice Guide in 2012. Since then, EU Member States and EFTA countries have made great progress in developing and implementing their strategies. This guide is updating the different steps, objectives and good practices of the original guide and analyses the status of NCSS in the European Union and EFTA area. The aim is to support EU Member States in their efforts to develop and update their NCSS. Therefore, the target audience of this guide are public officials and policy makers. The guide also provides useful insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders.

The guide presents six steps for the design and development of NCSS:

- Set the vision, scope, objectives and priorities
- Follow a risk assessment approach
- Take stock of existing policies, regulations and capabilities
- Set a clear governance structure
- Identify and engage stakeholders
- Establish trusted information-sharing mechanisms

In addition, fifteen objectives for the implementation of NCSS are described:

- Develop national cyber contingency plans
- Protect critical information infrastructure
- Organise cyber security exercises
- Establish baseline security measures
- Establish incident reporting mechanisms
- Raise user awareness
- Strengthen training and educational programmes
- Establish an incident response capability
- Address cyber crime
- Engage in international cooperation
- Establish a public-private partnership
- Balance security with privacy
- Institutionalise cooperation between public agencies
- Foster R&D
- Provide incentives for the private sector to invest in security measures

This guide proposes a national cyber security strategy lifecycle, with a special emphasis on the evaluation and maintaining phase. Suggestions for possible and indicative Key performance indicators (KPIs) for objectives of the strategy are described. In addition, the guide presents the status of implementation of NCSS among EU Member States and identifies gaps and challenges such as:

- Establish effective cooperation between public stakeholders
- Establish trust between public and private stakeholders
- Ensure adequate of resources
- Promote a common approach and awareness for privacy and data protection
- The implementation of vulnerability and risk analysis

The guide concludes with a set of recommendations on how to proceed with the development and maintenance of EU Member States' NCSS:

- Recommendation 1: Consider to include the provisions of the NIS Directive into the NCSS
- Recommendation 2: Consider prioritizing certain critical sectors
- Recommendation 3: Align or integrate CIIP with NCSS and national emergency management structures
- Recommendation 4: Extend the scope of international cooperation beyond international exercises
- Recommendation 5: Create a common understanding of concepts and terminology
- Recommendation 6: Approach and involve stakeholders at an early stage of development
- Recommendation 7: Gain situational awareness
- Recommendation 8: Develop requirements and measures per critical sector
- Recommendation 9: Enhance capabilities of public and private actors

# List of Figures

# List of Abbreviations

| ABBREVATION | DESCRIPTION |
|---|---|
| CSIRTs | Computer Security Incident Response Teams |
| CIIP | Critical Information Infrastructure Protection |
| CISO | Chief Information Security Officer |
| EFTA | European Free Trade Association |
| ENISA | European Union Agency for Network and Information Security |
| ICT | Information and Communications Technology |
| ISAC | Information Sharing and Analysis Centre |
| ISP | Internet Service Providers |
| KPI | Key Performance Indicator |
| MS | Member State(s) |
| NCP | National Cyber Contingency Plan |
| NCSS | National Cyber Security Strategy |
| NDA | Non-Disclosure Agreement |
| NIS | Network and Information Systems |
| PDCA | Plan-Do-Check-Act |
| PPP | Public-Private Partnership |
| R&D | Research and Development |
| SCADA/ICS | Supervisory Control and Data Acquisition/Industrial Control Systems |
| SOP | Standard Operating Procedures |

# 1. Introduction

During the last few decades new technologies, e-services and interconnected networks have become increasingly embedded in our daily life. Businesses, society, government and national defence depend on the functioning of information technology (IT) and the operation of critical information infrastructures (CIIs). Transportation, communication, e-commerce, financial services, emergency services and utilities rely on the availability, integrity and confidentiality of information flowing through these infrastructures.

As society becomes more and more dependent on IT, the protection and availability of these critical assets are increasingly becoming a topic of national interest. Incidents causing disruption of critical infrastructures and IT services could cause major negative effects in the functioning of society and economy. As such, securing cyberspace has become one of the most important challenges of the 21st century. Thus, cyber security is increasingly regarded as a horizontal and strategic national issue affecting all levels of society.

To meet current and emerging cyber security threats, EU Member States need to constantly develop and adapt their cyber security strategies. National cyber security strategies (NCSS) are the main documents of nation states to set strategic principles, guidelines, and objectives and in some cases specific measures in order to mitigate risk associated with cyber security. Following a high-level top-down approach, NCSS set the strategic direction for subsequent actions.

Cyber security is still a relatively new problem area for nation states and while some EU Member States are already drafting their second or third edition, others are still in the initial development phase. ENISA is supporting the efforts of EU Member States by providing guidelines on how to develop and update NCSS, analysing existing strategies and outlining good practices. ENISA's work on NCSS in the past include:

- NCSS: An Implementation Guide[1]
- National Cyber Security Strategies[2]
- An Evaluation Framework for NCSS[3]
- Incentives and barriers of the cyber insurance market in Europe[4]
- An online National Cyber Security Strategies Map, providing an overview of the status of NCSS in EU and EFTA countries[5]
- Training material for Cyber Security Specialists, covering four main areas: Technical, Operational, Setting up a CSIRT and Legal and Cooperation[6]
- Public Private Partnerships (PPPs) on European and national level for the resilience of CII[7]
- Cyber exercising activities, such as the Cyber Europe programme[8]
- Contingency planning and cyber crisis management[9]
- Good Practice Guide on Information Sharing[10]

[1] https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[2] https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[3] https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[4] https://www.enisa.europa.eu/publications/incentives-and-barriers-of-the-cyber-insurance-market-in-europe
[5] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map
[6] https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists
[7] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership
[8] https://www.enisa.europa.eu/topics/cyber-exercises?tab=details
[9] https://www.enisa.europa.eu/topics/cyber-crisis-management
[10] https://www.enisa.europa.eu/publications/good-practice-guide

- Awareness raising and training measures[11]

The aim of the present good practice guide is to provide a comprehensive overview of different steps and objectives in order to develop and implement NCSS. For this purpose, this guide presents the initial findings of the 2012 guide and complements them with current examples and good practices, as well as an overview of the status of EU Member States NCSS and final recommendations.

## 1.1 The European policy context

The main regulatory and policy statements governing activities in the cyber security strategy field are briefly summarised below.

### European Strategy for Cyber Security

At the time of writing, the European Strategy for Cyber Security is still under development. The text that follows is therefore a reflection of the current state of affairs and may well change. The goal of the initiative is to propose a comprehensive cyber security strategy for Europe.[12]

### EC proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market

The aim of the European Directive 1999/93/EC on a community framework for electronic signatures was the legal recognition of electronic signatures.[13] Assessing the need for secure and seamless electronic transactions as well as the shortcomings of the Directive, the European Commission adopted on 4 June 2012 a proposal for a Regulation on electronic identification and trusted services for electronic transactions in the internal market.[14]

### Directive on Attacks against information systems

The Council Framework Decision 2005 and its replacement Directive 2013/40 /EU have set a legal framework for attacks against information systems. The objectives of this framework are to approximate the criminal law of the EU Member States in this area. For this purpose, the Directive establishes definitions of criminal offenses and sanctions. Furthermore, cooperation between law enforcement agencies and EU Agencies and bodies such as Eurojust, Europol and its European Cyber Crime Centre, and ENISA shall contribute to this improvement through different measures such as the exchange of information.[15]

### Network and Information Security Directive

In order to strengthen critical infrastructure against various threats and to uphold the trust of the EU citizens, the European Commission has proposed the Network and Information Security Directive (NIS Directive) in 2013. In

[11] https://www.enisa.europa.eu/news/enisa-news/e-learning-platform-by-enisa-on-national-cyber-security-strategies
[12] European Commission (2012): Update on European Strategy for Cyber Security. Available online at http://www.europarl.europa.eu/document/activities/cont/201207/20120712ATT48826/20120712ATT48826EN.pdf
[13] European Parliament and the Council (1999): Directive 1999/93/EC on a Community framework for electronic signatures. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN
[14] European Commission (2015): Trust services. Available online at http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm
[15] European Parliament and the Council (2013): Directive 2013/40/EU on attacks against information systems. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN

December 2015, the European Parliament and the Council reached an agreement on the Commission's proposal. The European Parliament adopted the final Directive in July 2016 and it entered into force in August 2016.[16]

The aim of the NIS Directive is to improve the EU Member States' national cybersecurity capabilities, enhancing the cooperation between the Member States, the public and the private sector while also requiring companies in critical sectors to report major incidents to national authorities and to adopt risk management practices.

Article 7 of the Directive requires EU Member States to develop and adopt a national cyber security strategy (NCSS). The article also specifically names seven issues that shall be part of a NCSS. If needed, Member States can call upon ENISA to assists them in drafting a NCSS. Within three months after the adoption of their NCSS, EU Member States need to forward the strategy to the European Commission.

## 1.2 Scope and objectives

This guide aims to provide useful and practical recommendations to relevant public and private stakeholders on the development, implementation and maintenance of a cyber security strategy. More specifically to:

- ✓ Define the areas of importance of cyber security strategies.
- ✓ Help EU Member States to develop, manage, evaluate and upgrade their national cyber security strategy.
- ✓ Identify the challenges, the lessons learnt and the good practices from the NCSS practices followed by EU MS.
- ✓ Provide useful recommendations for policy and decision makers.
- ✓ Contribute to the Commission's efforts towards an integrated pan-European cyber security strategy.

## 1.3 Target audience

The target audience of this guide are public officials and policy makers: that is, those who usually lead and participate in the process of developing and implementing a NCSS. The guide also provides useful insights for the stakeholders involved in the lifecycle of the strategy, such as private, civil and industry stakeholders. Typical examples include policy makers, regulators, telecommunication providers and internet service providers (ISPs), online banks, utility companies, computer emergency response team (CERT) experts and others.

## 1.4 Methodology

ENISA conducted a first study on NCSS in 2012, which resulted in the "National Cyber Security Strategy: An Implementation Guide". The present guide is based on the initial results of the 2012 study and updated with new findings. For this purpose, a series of interviews with representatives of national cyber security authorities has been conducted. Invitations to participate in the study was send to the NCSS experts group and other MS representatives, responsible for the NCSS in their country. Interviews were conducted with 16 Member States and 1 EFTA representative of the following seventeen countries:

1. Austria
2. Belgium
3. Bulgaria
4. Croatia
5. Denmark
6. Estonia
7. Finland
8. France
9. Greece
10. Hungary
11. Ireland
12. Luxembourg
13. Malta
14. Slovenia

[16] European Parliament and the Council of the European Union (2016): Directive (EU) 2016/1148 of the European Parliament and of the Council. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

15. Spain
16. Sweden
17. Switzerland

The results of the interviews were complemented by desk research. Following completion of the interview and analysis phase, a mapping of the implemented objectives across the examined countries was created. As a final step, recommendations were prepared, which shall provide guidance for countries on how to continue with the development of their NCSS.

The results of this guide have been validated by the NCSS Working Group and presented at the Network and Information Security Workshop in Bratislava in October 2016.

## 1.5 How to use this guide

This guide can be used in a number of ways:

- ✓ As a practical, systematic guide for creating a new cyber security strategy.
- ✓ To align existing strategies with the requirements of the NIS Directive.
- ✓ As an incentive for enhancing or complementing parts of an existing NCSS.
- ✓ As a benchmark for checking the effectiveness of measures in existing NCSS.
- ✓ As a basis for improving the maintenance of existing NCSS.
- ✓ To gain an overview of the status of NCSS in European countries.

The guide describes:

- ✓ A simplified lifecycle model for developing, evaluating and maintaining a national cyber security strategy.
- ✓ The main steps when developing a NCSS.
- ✓ The main objectives of implementing and executing a NCSS.
- ✓ Tasks and examples for each step and objective.
- ✓ Gaps and challenges that countries were facing in the implementation of different measures.
- ✓ Recommendations for the future development of NCSS.

# 2. National cyber security strategy lifecycle

For governing national cyber security strategies, ENISA developed the NCSS lifecycle. In order to check and continuously improve the strategy and related policies as well as its implementation through measures, actions and processes, we recommend applying a lifecycle approach:

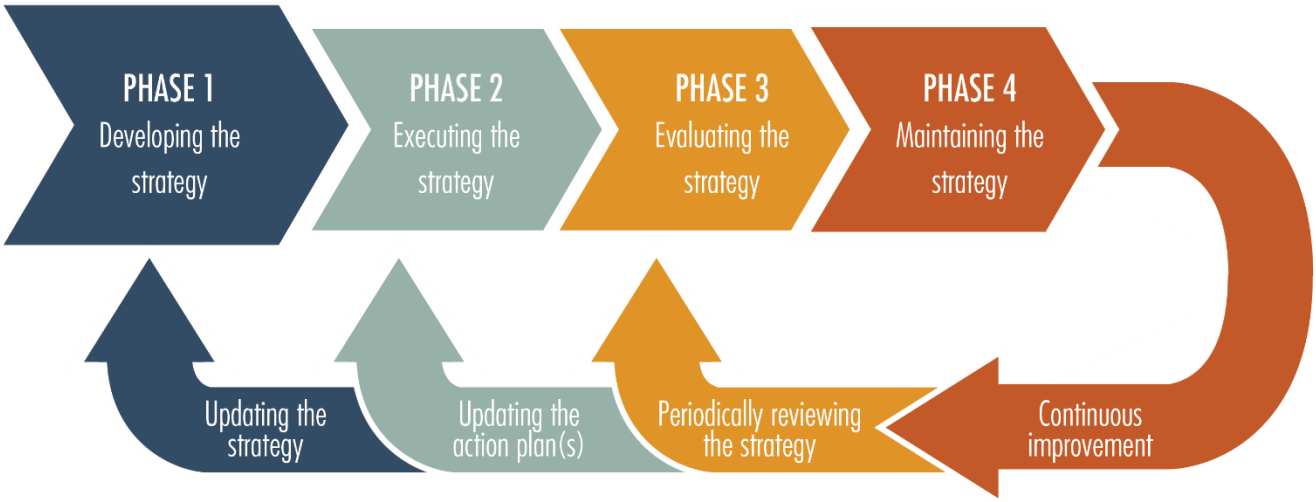


**Figure 2-1 – NCSS lifecycle**

The original 2012 "National Cyber Security Strategy: An Implementation Guide" was focused on Phase 1 and Phase 2 of the lifecycle approach and gave advice and recommendations on how to develop and execute a NCSS. Since then, ENISA has been focusing on Phase 3, the evaluation and adjustment of strategies for continuous improvement. To this end, ENISA published an evaluation framework for cyber security strategies in 2014.[17] The guide aims to be a pragmatic evaluation tool and presents a set of possible key performance indicators (KPIs).

The present guide includes the initial findings of the 2012 guide and complements them with current examples and good practice. In addition, the guide includes Phase 3 and Phase 4 of the NCSS lifecycle. Phase 3 is covered by analysing and evaluating existing NCSS of EU Member States and EFTA countries. For this purpose, we identified challenges and gaps that countries were facing in implementing NCSS and provide an overview of the status of NCSS in Europe. In order to help countries to maintain and adjust existing NCSS, the guide also offers a set of recommendations on how to improve and update their strategies.

[17] ENISA (2014): An evaluation framework for Cyber Security Strategies. Available online at https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

# 3. Design and develop a national cyber security strategy

This chapter aims at providing guidance to the steering and editorial teams of the strategy on the main steps that should be considered during the development phase.

Each sub-chapter puts the focus on specific steps that require attention and should be considered during the drafting of NCSS. Examples for the integration of the steps in NCSS are provided at the end of every chapter. If an example is from a publicly available source, a reference is provided. In cases where examples are based on confidential interviews with EU Member States' officials, no references are provided.

## 3.1 Set the vision, scope, objectives and priorities

A strategy can be defined as a plan of actions designed to achieve a long-term or overall aim.[18] The aim of a cyber security strategy is to increase the global resilience and security of national ICT assets, which support critical functions of the state or of the society as a whole. Setting clear objectives and priorities is thus of paramount importance for successfully reaching this aim.

Typical **tasks** to consider in this step are listed here:

- ✓ Define the vision and scope that set the high-level objectives to be accomplished in a specific time frame (usually 5-10 years).
- ✓ Define the business sectors and services in scope for this strategy.
- ✓ Prioritise objectives in terms of impact to the society, economy and citizens (see chapter 4 for examples of potential objectives).
- ✓ Define a roadmap for the implementation of the strategy, which may involve the following steps.
    - Define concrete activities that would meet the objectives of the strategy.
    - Develop a governance framework for the implementation, evaluation and maintenance of the strategy.
    - Develop a master plan for the implementation of the strategy.
    - Develop concrete action plans for each activity.
    - Define the evaluation of the strategy and its main actions (e.g. which key performance indicators (KPIs)) will be performed and by whom.

**An example: National interests and strategic objectives in the Polish NCSS**

*The present document identifies national interests and strategic objectives in the domain of security, in accordance with principles and values comprised in the Constitution of the Republic of Poland. It determines the national security capacities, assesses Poland's security environment in its global, regional and national dimension and projects its development trends. It presents actions of the state which are necessary to fulfil the defined interests and objectives, and also points out directions and ways of preparation of the national security system.*[19]

**An example: Priority areas in the Cyprian NCSS**

*The strategic response of the Republic of Cyprus to the previously mentioned threats can be split into a*

[18] Oxford University Press (2012): Oxford English Dictionary, 7th Edition.

[19] National Security Bureau (2014): National Security Strategy of the Republic of Poland. Available online at http://en.bbn.gov.pl/download/3/1314/NSSRP.pdf

*number of priority areas that have been identified for the optimal protection of critical information infrastructures.*

- *coordination of governmental stakeholders to ensure correct and efficient cooperation,*
- *creation of a comprehensive legal framework by the competent authorities of the state, that covers all aspects of network and information security, including cybercrime and the protection of personal data,*
- *formulation of technical and organisational measures and procedures to harden the security of relevant hardware, software and physical spaces, to the required degree,*
- *development of the necessary skills, training and awareness in security topics, for those that are directly involved and also for the public,*
- *productive collaboration between the public and private sector, on both the national and international level,*
- *creation or adaption of the necessary structures and instruments within the competent authorities and the more generally the Cyprus Government, to secure the demands and capabilities of immediate incident response.*[20]

## 3.2 Follow a risk assessment approach

One of the key elements of a cyber security strategy is the national risk assessment, with a specific focus on critical information infrastructures. Risk assessment is a scientific and technologically based process consisting of three steps: risk identification, risk analysis and risk evaluation.[21] The scope of the assessment is to coordinate the use of resources and to monitor, control, and minimise the probability and/or impact of unfortunate events that might put at risk the critical services and ultimately the objectives of the vision.

Risk assessments can provide valuable information for developing, executing and evaluating a strategy. The assessment can be conducted on different levels. Risk assessment on a national level allows gaining a holistic understanding about risk to the nation as a whole. By carrying out a national risk assessment and aligning the objectives of the strategy with national security needs, it is possible to focus on the most important challenges with regard to cyber security. Sectorial risk assessment allows considering more sector-specific risks to critical infrastructure and service providers.

Risk assessment can be conducted by a national authority, sectoral authorities or by operators of CI on different levels. Information sharing between the different entities ensures that agencies can learn from other perspectives (see 3.6 Establish trusted information-sharing mechanisms).

In most cases, governments and companies adopt an all-hazard approach (i.e. incorporating all kinds of cyber threats such as cyber crime, hacktivism, technical failures or breakdowns) when assessing the risks at national level or for their organisation. For more information on risk assessments, please check ENISA's publication *National-level Risk Assessments. An Analysis Report.*[22]

Typical **tasks** to consider in this step are listed below:

[20] Office of the Commissioner of Electronic Communications & Postal Regulation (2012): Cybersecurity Strategy of the Republic of Cyprus. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf

[21] ENISA (2016): Current Risk. Glossary. Available online at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

[22] ENISA (2013): National-level Risk Assessments. An Analysis Report. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report

- ✓ Agree on a risk assessment methodology to use; if this is not possible, tailor an existing one to the specific needs of national and sectorial risks.
- ✓ Task a national authority or sector-specific authorities with conducting risk assessment.
- ✓ Design and follow an approach to risk identification and assessment (e.g. all-hazard approach).
- ✓ Develop a method for the identification of critical (information) infrastructure

**An example: Risk assessment in Switzerland**

*Identification, analysis and evaluation*

*The Federal Administration and the 28 identified critical sub-sectors are obliged to conduct a risk assessment according to the NCS. The risk analysis process is as follows: 1. Assessment of critical processes, 2. Assessment of critical systems, 3. Assessment of vulnerabilities, 4. Assessment of risks. The implementation of risk assessment is decentralised, but the Swiss government is offering strong support to the private sector.*

*Performance targets and planning*

*After the risk assessment analysis has been conducted, a catalogue of corresponding security measures is identified and implemented. This process is constantly overseen and adapted, if necessary.*

**An example: Different levels of risk analysis in Spain**

*Spain conducts risk analysis on different levels: The strategic-political level, the operational level and the tactical-technical level. These levels act in a coordinated manner to obtain an overview of cybersecurity risks.*

***Strategic-political level:** The **National Security Strategy** is the framework of the National Security Policy. It contains the analysis of the strategic environment, particular risks and threats to the security of Spain. Therefore, it is the first step in risk analysis. In addition, the **National Cyber Security Council** (part of the National Security Council) assesses risks and threats, analyses possible scenarios of crisis, studies its possible evolution, develops and updates response plans.*

***Operational level:** This level includes the situation monitoring by various bodies and agencies with cybersecurity skills on an operational level, such as the National Intelligence Centre (CNI), Joint Operation Command of the Armed Forces of Spain or the Secretary of State for Security from the Ministry of Interior.*

***Tactical-technical level:** It includes monitoring the situation by various bodies and agencies responsible for cybersecurity at the tactical-technical level. Relevant authorities on this level are the Spanish Joint Cyber Defense Command with a specialized Computer Emergency Response Team (CERT), the National Centre for Critical Infrastructure Protection (CNPIC), the Spanish National Institute of Cybersecurity (INCIBE) and the National Cryptologic Centre.*

## 3.3 Take stock of existing policies, regulations and capabilities

During the design and development process of a NCSS, it is necessary to identify and take into account EU and other international requirements. This will help to align the NCSS with international standards and to identify important gaps.

Typical **tasks** to consider in this step include the following:

- ✓ Establish existing policies developed over the years in the area of cyber security (i.e electronic communications, data protection, information security); bear in mind that cyber security is/should be part of an overall national security policy framework.

- ✓ Establish EU policies, directives and requirements with regard to cyber security.
- ✓ Align or differentiate your cyber security strategy with other overlapping areas, such as CIP or crisis management.
- ✓ Identify all regulatory measures applied in different sectors and their impact, so far, in improving cyber security (e.g. mandatory incident reporting in the electronic communications sector).
- ✓ Identify existing soft regulatory mechanisms (e.g. public and private partnerships) and assess the extent to which these have achieved their goals.
- ✓ Analyse the roles and responsibilities of existing public agencies mandated to deal with cyber security policies, regulations and operations (i.e energy regulators, electronic communications' regulators, data protection authorities, national cyber crime centres); identify overlaps and gaps.
- ✓ When updating the NCSS make the strategic evolution transparent: What kind of new/updated objectives are part of the new NCSS and why?

**An example: From NCSS1 to NCSS2 in the Netherlands**

*The Dutch NCSS2 describes and lists the major differences between its NCSS1 and its updated NCSS2:*[23]

| NCSS1 | NCSS2 |
|---|---|
| Public-private partnership | Private-public participation |
| Focus on structures | Focus on networks / strategic coalitions |
| Formulation of multi-stakeholder model | Clarifying the relationships between the various stakeholders |
| Capacity-building in the Netherlands | Capacity-building both in the Netherlands and abroad |
| General approach: deploy wide capacity for resilience-increasing measures | Risk-based approach: balance between protection of interests, threat to interests and acceptable risks in society |
| Formulation of fundamental principles | Presentation of (policy) vision |
| From ignorance to awareness | From awareness to capability |

## 3.4 Set a clear governance structure

The cyber security strategy will succeed only if a clear governance framework is in place. A governance framework defines the roles, responsibilities and accountability of all relevant stakeholders. It provides a framework for dialogue and coordination of various activities undertaken in the lifecycle of the strategy.

A public body or an interagency/interministerial working group should be defined as the coordinator of the strategy with the overall responsibility for the strategy lifecycle and the strategy documentation itself. The structure of the coordinating entity, its exact responsibilities and its relationships with the other stakeholders should be clearly defined.

[23] National Coordinator for Security and Counterterrorism (2013): National Cyber Security Strategy 2. From awareness to capability. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-1/at_download/file

Different governance structures are possible to govern cyber security. A centralised approach is usually characterised by a central cyber security authority with wide responsibilities and competencies across sectors. Decentralised approaches are characterised by a strong degree of cooperation between public agencies. This approach is often motivated by the principle of subsidiarity. Countries have also developed different relationships with the private sector. Some countries have established co-regulation in the issue area of cyber security through institutionalised forms of cooperation such as public-private partnerships. Other countries have developed new laws in order to regulate the private sector. For more information on governance profiles, please check ENISA's work on the protection of CII.[24]

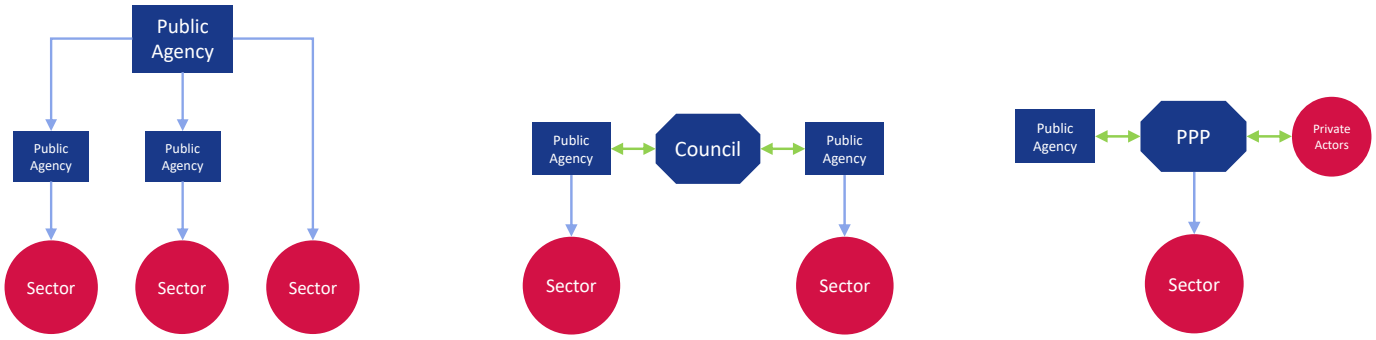


**Figure 3-1 – Governance structures**

The selected approach and the relating governance structure should be clearly defined and reflected in the national cyber security strategy together with the expected benefits.

Typical **tasks** to consider in this step are listed here:

- ✓ Define who is ultimately responsible for the management and evaluation of the strategy; usually some kind of cyber security coordinator is responsible for managing the cyber security strategy.
- ✓ Define the management structure i.e an advisory body that advises the cyber security coordinator of the strategy. Specify the governmental and private parties taking part in this structure. Try to cover the widest spectrum of stakeholders involved.
- ✓ Define the mandate (e.g. roles, responsibilities, processes, decision rights) and tasks of this advisory body (e.g. it manages the national risk management, assesses and prioritises emerging threats, responds to critical situations, manages the progress of the strategy, engages relevant stakeholders, fosters international cooperation etc.).
- ✓ Define or confirm the mandate and tasks of the entities responsible for initiating and developing cyber security policy and regulation; explain how these interact with and/or contribute to the advisory body.
- ✓ Define the mandate and tasks of the entities responsible for collecting threats and vulnerabilities, responding to cyber attacks, strengthening crisis management and others; explain how these interact with and/or contribute to the advisory body.
- ✓ Properly analyse and define the role of existing, national cyber security and incident response teams (CERT) in both public and private sectors. The national/governmental CERT may be tasked with monitoring activities, trusted information sharing, providing news on emerging threats and other critical information infrastructure protection activities.

[24] For more information on governance profiles, please see: ENISA (2016): Stocktaking, Analysis and Recommendations on the Protection of CIIs. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

**An example: ANSSI in France**

*In July 2009, the French Network and Information Security Agency (ANSSI) was created. ANSSI is an inter-ministerial agency attached to the Prime Minister's office and acts under the strategic guidance of SGDSN. The agency's role was strengthened in 2011, when it was declared the national authority for the defence of information systems.*

*ANSSI has been empowered to define implementing and enforcement measures of the French CIIP law ("Loi de programmation militaire 2014-2019") and is currently working with the government as well as with private entities to define the application conditions of this law.*[25]

**An example: Inner and Outer Circle in Austria**

*There are several relevant agencies in Austria, which are part of an "operative coordination structure". The governance model follows a cooperative and decentralised approach.*

*The Federal Chancellery of Austria and the Federal Ministry of the Interior share responsibility on a strategic-political level.*

*On an operational level, the operative coordination structure is divided between an "Inner circle" and an "Outer circle". The Inner Circle includes several public agencies, notably the Cyber Security Center, the Cyber Defense Center, GovCERT, MilCERT and the Cyber Crime Competence Center (C4). The Outer circle includes private organisations, such as the several sector-specific CERTs and the national CERT (CERT.at)*

**An example: Decentralised governance in Sweden**

*Sweden is a good example for a country that follows a decentralised approach in CIIP. The country uses a "system perspective", which means that the main tasks of CIIP, such as the identification of vital services and critical infrastructures, the coordination and support of operators, regulatory tasks as well as measures for emergency preparedness are the responsibility of different agencies and municipalities. Among these agencies are the Swedish Civil Contingencies Agency (MSB), the Swedish Post and Telecom Agency (PTS), and several Swedish Defence, Military and law enforcement agencies.*

*In order to coordinate the actions between the different agencies and public entities, the Swedish government has developed a cooperative network comprised of authorities "with specific societal information security responsibilities". This Cooperation Group for Information Security (SAMFI) consists of representatives of the different authorities and meets several times a year to discuss issues related to national information security. SAMFI's subject areas are mainly to be found in political-strategic areas and cover topics such as technical issues and standardization, national and international development in the field of information security, or management and prevention of IT incidents.*[26]

## 3.5 Identify and engage stakeholders

A successful cyber security strategy requires proper cooperation between public and private stakeholders. Identifying and engaging stakeholders are crucial steps for the success of the strategy. Public stakeholders usually

[25] ENISA (2016): Stocktaking, Analysis and Recommendations on the protection of CIIs. Available online at https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis
[26] ibid.

have a policy, regulatory and operational mandate. They ensure the safety and security of the nation's critical infrastructures and services. Selected private entities should be part of the development process because they are likely the owners of most of the critical information infrastructures and services.

Typical **tasks** to consider in this step include the following.

- ✓ Identify public stakeholders responsible for initiating and designing cyber security policy and regulation e.g. national telecommunications regulator, centre for the protection of national infrastructures etc.
- ✓ Engage both public and private stakeholders in the process by clearly defining their roles and responsibilities (e.g. private stakeholders protect their infrastructures and there is a joint responsibility with regard to protecting national security).
- ✓ Involve the right stakeholders at the right time in the process of developing the strategy. Stakeholder involvement is necessary from a strategic point of view to gain commitment for executing the strategy at a later stage.
- ✓ Explain how and why these stakeholders contribute to the objectives of the strategy, the individual tasks and the actions plans (e.g. pursue a collaborative approach together with critical infrastructure owners and critical service providers in assessing threats and risks).
- ✓ Assign to the government the role of a facilitator. The government can facilitate activities on a national level, such as information-sharing, (international) cooperation and risk management.
- ✓ Involve top-level representatives in order to create ownership and assign an alternate for each representative.
- ✓ Define the appropriate incentives that allow private and public stakeholders to participate in the process (e.g. no costly regulations). Take into account the possible different or even conflicting interests of the public and private sector.

**An example: Early approach of private stakeholders in Austria**

*The CI-operators in Austria were proactively approached at a very early stage. Since the new NIS-Directive required the drafting of appropriate laws in Austria, private stakeholders were giving the means to voice the concerns and ideas during the process of drafting the new law.*

**An example: Bottom-up approach in Estonia**

*In order to reach an understanding about the need for an overarching document for cyber security, stronger communication between the relevant stakeholders was necessary. For this purpose, a bottom up approach was applied. This approach included regular working groups with representatives of relevant public authorities in order reach a common understand of the needed objectives.*

## 3.6 Establish trusted information-sharing mechanisms

Information-sharing among private and public stakeholders is a powerful mechanism to better understand a constantly changing environment. Information-sharing is a form of strategic partnership among key public and private stakeholders. Owners of critical infrastructures could potentially share with public authorities their input on mitigating emerging risks, threats, and vulnerabilities while public stakeholders could provide on a 'need to know basis' information on aspects related to the status of national security, including findings based on information collected by intelligence and cyber-crime units. Combining both views gives a very powerful insight on how the threat landscape evolves.

Typical **tasks** to consider in this step include the following:

- ✓ Properly define the information-sharing mechanism and the underlying principles and rules that govern the mechanism (e.g. non-disclosure agreements, traffic-light protocol, antitrust rules)

- ✓ Follow a sector approach to information sharing (e.g. one information-sharing platform for ISPs, one for energy etc.). Make sure that there is enough information flow among the different information-sharing schemes.
- ✓ Encourage cross sector communication, not only sector focused information sharing. As there are many interdependencies between sectors (banking sector cannot work without energy support for example), cross sector information exchange needs to be considered.
- ✓ Focus on strategic issues and critical threats and vulnerabilities (e.g. major/critical disruptions).
- ✓ Provide the appropriate incentives for stakeholders (mostly for private ones) to participate and share sensitive information (sharing with the community the results of the analysis), e.g. by providing unique, strategic insights to policy and decision-makers.
- ✓ Make sure that the right experts with the right profile take part in the scheme. Normally participants are high-level security experts (e.g. CISOs) able to share information at corporate level.
- ✓ Decide whether experts from law enforcement, intelligence, national/governmental CSIRTs and relevant regulatory bodies should be present.
- ✓ Keep the size of the information-sharing scheme relatively small to allow trust among experts to flourish.
- ✓ Organise regular (face-to-face) meetings to share sensitive information. Government should facilitate the process and provide logistical support. The initiative could be chaired both by the public sector and industry to symbolise the joint responsibility of the two stakeholders' categories.
- ✓ Identify other relevant European or international trusted information-sharing communities and decide whether to engage with them to expand your level of understanding, or not to.
- ✓ Update the national risk registry and distribute the collected information, in an anonymous way, to appropriate targeted users through the early-warning systems.

**An example: The Czech National Security Agency (NSA)**

*The Czech National Security Agency (NSA) acts as the main information hub. It also coordinates the different public and private CERTs in case of an emergency. The NSA supports and advises operators of CII in emergency response and provides forensic analysis if requested.*

*The NSA conducts seminars for operators of CII and advises them on legal obligations, the role of the NSA and the responsibilities of operators. In addition, an E-learning platform is currently under development. The long-term goal is to build an information platform, which should also include sectoral information for operators.*

**An example: The Dutch National Response Network and the National Detection Network**

*In 2014, the National Response Network (NRN) and the National Detection Network (NDN) were launched. The NRN is a collaboration between the NCSC and public-private ICT response organisations from various sectors. Within the NRN knowledge and experiences can be shared between the different stakeholders and response capacities can be organised. The NDN serves as an information platform, where information about threats and digital dangers are exchanged.*[27]

**An example: The Swiss Reporting and Analysis Centre for Information Assurance (MELANI)**

*MELANI is responsible for providing subsidiary support for information assurance within the critical infrastructure. It acts as a centralised information hub by receiving information on incidents and threats from private operators and public agencies, evaluating these and passing the results on to the operators of CII. Often, the information shared by MELANI comes from publically not available sources such as*

[27] National Cyber Security Centre (2016): National Detection Network. Available online at https://www.ncsc.nl/english/Cooperation/national-detection-network.html

*Intelligence Services, Police Entities or technical analysis. MELANIs constituency consists of around 200 enterprises that operate critical infrastructure.*

# 4. Implementation of the national cyber security strategy

This chapter aims at providing guidance to relevant actors that lead and participate in the execution and implementation of a NCSS. Examples for relevant actors are public officials, policy makers, but also private actors and civil society.

Each sub-chapter will focus on a non-exhaustive list of tasks required to meet the overall objective. Examples and good practices for reaching these objectives and tasks are provided at the end of every chapter. If an example is from a publicly available source, a reference is provided. In cases where examples are based on confidential interviews with EU Member States' officials, no references are provided. The objectives will outline the core of the overall 'national philosophy' on cyber security.

## 4.1 Develop national cyber contingency plans

National cyber contingency plans (NCPs) are the interim structures and measures for responding to, and recovering services following, major incidents that involve critical information infrastructures (CIIs).[28] A national cyber security contingency plan should be part of or aligned with overall national contingency plans. It is also an integral part of the cyber security strategy.

The **objectives** of a NCP are to:

- ✓ Present and explain the criteria that should be used to define a situation as a crisis.
- ✓ Define key processes and actions for handling the crisis.
- ✓ Clearly define the roles and responsibilities of different stakeholders during a cyber-crisis.

An NCP should be developed within a lifecycle. In essence, the lifecycle is a quality assurance and management cycle for such plans. Following that, the main **tasks** for developing the NCP are the following:

- ✓ Perform an initial risk assessment, which will cover the process of identifying threats and vulnerabilities and their potential impact and will define a set of priorities.
- ✓ Engage the relevant stakeholders in the process and make sure their roles and responsibilities are clear and not overlapping.
- ✓ Develop the standard operating procedures (SOPs) for use by all relevant stakeholders during different crises.
- ✓ Develop the necessary cooperation and response framework to be used, e.g. capabilities, procedures, non-disclosure agreements (NDAs), etc.
- ✓ Define the procedures to be used for dealing with the media during emergency situations.
- ✓ Test, evaluate and adjust procedures, capabilities and mechanisms; one proven way of doing this is through cyber exercises.
- ✓ Train the personnel responsible for offering the capabilities.
- ✓ Organise and execute exercises that will evaluate the existing standard operating procedures, roles and responsibilities and communication mechanisms.
- ✓ Review the contingency plan taking and take lessons learnt from cyber exercises into consideration.

[28] ENISA (2012): Good Practice Guide on National Contingency Plans for CIIs, available on request.

**An example: National Crisis Management Plan in Poland**

*The Polish National Crisis Management Plan lays out the general roles and responsibilities during a crisis situation. The Council of Ministers holds the political responsibility and will be advised by a Government Crisis Management Team in case of national emergency. The Team shall be composed of different ministers relevant to the kind of crisis. In case of an emergency related to CII, the Ministry of Administration and Digitization will take a leading role in advising other Ministries and the Council of Ministers in crisis situations.*

## 4.2 Protect critical information infrastructure

Critical information infrastructure protection (CIIP) is an integral part of many cyber and information security strategies. Cybersecurity covers a broad spectrum of ICT-related security issues, of which the protection of CII is an essential part.

The **objectives** of CIIP are to:

- ✓ Identify critical information infrastructure.
- ✓ Identify and mitigate relevant risks to CII.

Typical **tasks** include the following:

- ✓ Define and identify critical sectors. Typical examples include energy, health, transport, finance, telecommunications, etc.
- ✓ Develop a method for the identification of critical infrastructure.[29]
  - Identify assets and services critical to the proper functioning of the society and economy.
  - Identify owners and providers of CI.
- ✓ Involve relevant stakeholders. This includes, but is not limited to:
  - Involve specific critical infrastructure owners instead of allocating responsibilities to a specific sector. By allocating responsibilities to individual companies, these can be held responsible and/or even accountable for not taking proper security measures.
  - Include civil society (end users, civilians) in executing the strategy from an awareness point of view. By raising awareness at a national level, citizens will better understand cyber security risks and this will enable them to proactively take measures to lessen or mitigate risks.
  - Involve ministries with responsibility for security, safety, crisis management, such as defence, interior, foreign affairs, justice, national telecommunication regulator, data protection authority, and cyber crime unit in developing the strategy.
  - Involve existing national CSIRTs or CSIRT communities (of companies) as they may be a critical part of the information-sharing capabilities on a national level.
  - Involve national interest groups in order to incorporate the interest of different stakeholder groups.
- ✓ Establish a set of sector specific protection plans. Activities in this task might include the following.
  - Assess all risks affecting the critical assets, prioritise them according to their impact[30] and calculate the probability of being realised.
  - Engage the right private sector stakeholders, share with them their risk assessments and correlate them with your findings.

[29] For details on different methodologies for the identification of CII, please see: ENISA (2015): Methodologies for the identification of Critical Information Infrastructure assets and services. Available online at https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

[30] Various metrics can be used for the impact assessment e.g. monetary units, people affected.

- Decide which risks you mitigate, accept, avoid or share and document the relating measures (be clear why you make these decisions).
- Develop a national risk registry to store the identified risks.
- Define a recurring process for continually monitoring threats and vulnerabilities and updating the national threat landscape.

- Extend to cross sector collaboration based on identified interdependencies.

**An example: The German IT-Security Act**

*The IT Security Act provides a definition of critical infrastructure. A methodology for the identification of critical infrastructure has been developed. The German federal ministry of the interior is applying this methodology in an administrative order (BSI-KRITIS-Verordnung) that further defines which infrastructures are critical and affected by the IT Security Act.*[31]

**An example: The Spanish National Centre for Critical Infrastructure Protection (CNPIC)**

*The National Centre for Critical Infrastructure Protection (CNPIC) is the organism in charge of promoting, coordinating and supervising all critical infrastructure protection (CIP)-related activities for which the Secretariat of State for Security is competent at national level.*

*The main objective of the Centre is promoting and coordinating the mechanisms needed to guarantee the security of the infrastructures that supply services that are essential to our society, encouraging to this end all the agents of the system to take part in their respective fields of competence. By means of all these efforts, the CNPIC promotes a security model based on mutual trust, creation a public-private partnership that will allow minimizing the vulnerabilities of critical infrastructure in Spain.*

*Operators designated as being critical by the National CIP Commission will be part of the CIP System and will be responsible for optimizing the protection of the critical infrastructure they manage*

**An example: The Swiss Critical Infrastructure Inventory**

*The National CIP Strategy of 2012 identifies 28 sub-sectors within ten sectors that are assessed as being of critical national importance. A methodology has been developed to prioritize sub-sectors. A key element is the assessment of the damage to be expected from a failure of the critical sub-sectors, determined by the effects on other sub-sectors (interdependencies), on the population, and on the economy. Eight subsectors of overriding importance in the field of CIP were identified. By the end of 2012, a CI Inventory was assembled with a refined methodology.*[32]

## 4.3 Organise cyber security exercises

Exercises enable competent authorities to test existing emergency plans, target specific weaknesses, increase cooperation between different sectors, identify interdependencies, stimulate improvements in continuity planning,

[31] IT-Security Act (2015). Available online at https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile

[32] Bundesamt für Bevölkerungsschutz BABS (2012): Nationale Strategie zum Schutz kritischer Infrastrukturen. Available online at http://www.babs.admin.ch/de/aufgabenbabs/ski.html

and generate a culture of cooperative effort to boost resilience. Cyber exercises are important tools to assess preparedness of a community against natural disasters, technology failures, cyber-attacks and emergencies.

Typical **objectives** for this are to:

- ✓ Identify what needs to be tested (plans and processes, people, infrastructure, response capabilities, cooperation capabilities, communication, etc.).
- ✓ Set up a national cyber exercise planning team, with a clear mandate.
- ✓ Integrate cyber exercises within the lifecycle of the national cyber security strategy or the national cyber contingency plan.

Typical **tasks** to consider in this step include the following:[33]

- ✓ Develop a mid-term vision with concrete objectives to be achieved.
- ✓ Identify the relevant public and private sector stakeholders to be involved in the process.
- ✓ Assess the impact of one or the series of cyber exercises and update your vision to meet the needs of the cyber security strategy.

**An example: Cross-sectoral cyber exercises in Austria**

*Cross-sectoral cyber exercises for SMEs will be organised and held at periodic intervals. Specific sectors of SMEs should be allowed to participate in governmental cross-sectoral cyber exercises upon request.*[34]

**An example: International and sector-specific exercises in Sweden**

*Sweden conducted several exercises with regard to CIIP and Cyber Security. The SAMÖ 2008 simulated an IT attack against financial systems. In 2012, the National Cyber Security Exercise NISÖ was conducted. Sweden was also part international cyber security exercises such as Cyber Storm III (September 2010) or the multi-national International Watch and Warning Network Exercise 2013, both organised by the United States.*

*In addition, sector-specific exercises with a focus on information security are conducted on a regular basis. The National Telecommunications Coordination Group (NTSG) organises exercises every two years with the eight largest telecommunications operators and the PTS.*

## 4.4 Establish baseline security measures

All relevant public and private organisations should take necessary measures to protect their information infrastructure from threats, risks and vulnerabilities identified after the completion of the national risk assessment. Baseline security requirements for a given sector define the minimum security level that all organisations in that

[33] For more information on this topic, please check the following ENISA publications: ENISA (2009): Good Practice Guide on National Exercises. Enhancing the Resilience of Public Communications Networks. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide; ENISA (2012): National and International Cyber Security Exercises: Survey, Analysis & Recommendations. Available online at https://www.enisa.europa.eu/publications/exercise-survey2012; ENISA (2012): Cyber Europe 2012 – Key Findings Report. Available online at https://www.enisa.europa.eu/publications/cyber-europe-2012-key-findings-report; ENISA (2015): ENISA Cyber Europe 2014 – After Action Report. Available online at https://www.enisa.europa.eu/publications/ce2014-after-action-report; ENISA (2015): Latest Report on National and International Cyber Security Exercises. Available online at https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

[34] Federal Chancellery of the Republic of Austria (2013): Austrian Cyber Security Strategy. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/AT_NCSS.pdf

sector should comply with. Such requirements can be based on existing security standards or frameworks and good practices widely recognised by the industry.

Defining a minimum set of security measures is a complex exercise that should take into account the following aspects: the different level of maturity among the stakeholders, the differences in terms of the operational capacity of each organization and the different standards existing in each critical sector under consideration.

Typical **objectives** of this phase should be to:

- ✓ Harmonise the different practices followed by the organizations in both the public and the private sector.
- ✓ Create a common language between the competent public authorities and the organisations.
- ✓ Enable different stakeholders to check and benchmark their cyber security capabilities.
- ✓ Share information about the cyber security good practices in every different industry sector.
- ✓ Help the stakeholders to prioritise their investments on security.

Typical **tasks** to consider include the following:

- ✓ Identify, analyse, and adopt appropriate, sector-wide minimum security measures to manage the threats associated with the incidents.
- ✓ Continuously review and then update the existing set of measures.
  - Identify the security measures that already described in the existing regulatory documents.
  - Identify the information security threats and then map these threats to the existing measures.
  - Identify the gaps and derive mitigation measures from the existing technical standards (e.g. ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz). Where gaps are found, enhance the list of measures by taking into account the opinion of the experts and the relevant standards.
  - Update the relevant regulatory texts with the new measures.
- ✓ Create maturity self-assessment tools and encourage the stakeholder to use them.
- ✓ Set up internal and joint procedures to review continuously the implementation of adopted measures, e.g. through mandating information security audits to competent authorities based on the list of the minimum measures.
- ✓ Update the baseline requirements based on reported incidents of significant impact.
- ✓ Define the nature of the baseline requirements: Define if the baselines are recommendations or mandatory.

**An example: IT Security Act in Germany**

*According to the IT Security Act, operators of CII are obligated to implement appropriate technical and organisational measures in order to ensure the security of their information systems that are necessary for the availability of their critical services. For this purpose, operators shall take into account international, European and national norms and standards. In addition, sector specific security standards may be implemented.*

*Furthermore, operators are obligated to establish a contact point within their organisation.*[35]

**An example: A CIIP law in France**

[35] IT-Security Act (2015): Available online at https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile

*All OIVs are required to comply with the obligations listed in Article 22 of the French CIIP law ("Loi de programmation militaire 2014-2019"). These obligations include compliance with rules for the protection of information systems set by ANSSI on behalf of the Prime Minister. These rules can be technical or organisational.*

*According to the CIIP law, OIVs are obligated to report cybersecurity incident notifications to ANSSI. The nature of incidents to be notified will be specified by sectorial orders.*

*During major crisis that threaten the security of information systems of critical infrastructure, the Prime Minister may decide on additional measures that OIVs would have to implement.*

*According to the CIIP Law, OIVs are obligated to undergo cybersecurity audits, performed either by ANSSI or a service provider qualified by ANSSI. Audit reports are classified and provided to ANSSI.*[36]

## 4.5 Establish incident reporting mechanisms

Reporting security incidents plays an important role in enhancing national cyber security. The more a person knows about major incidents the better they can understand the threat environment. Incident reporting and analysis helps in adjusting and tailoring the list of security measures, mentioned in the previous section, to the changing threat landscape. This way, the national preparedness, response and recovery capabilities are enhanced.

Typical **objectives** are:

- ✓ Gain knowledge on the overall threat environment.
- ✓ Assess the impact of incidents (e.g. security breaches, network failures, service interruptions).
- ✓ Gain knowledge on existing and new vulnerabilities and types of attacks.
- ✓ Update security measures accordingly.
- ✓ Implement NIS Directive provisions on incident reporting[37]

Typical **tasks** of this activity include the following:

- ✓ Identify the need for incident reporting by:
  - Deciding whether there are incident reporting schemes within the already existing on national, European and international cyber security level and identify gaps and needs that are not addressed and that a new scheme will have to cover or satisfy.
  - Identifying the types of incidents to be reported and the purpose of the new scheme.
  - Outlining the reporting requirements, especially the scheme's constituency (the potential reporting parties), the reporting obligation and the thresholds beyond which incidents should be reported.
- ✓ Engage in cooperation with the involved parties by:
  - Making use of existing arrangements and resources.
  - Formulating the value proposition of the scheme.
  - Raising awareness of the threats.
  - Building trust with the participants and addressing the private stakeholders' concerns.
  - Drafting specific laws or regulation.
- ✓ Set the reporting procedures by:
  - Setting reporting requirements.
  - Defining the prioritisation of incidents.
  - Establishing follow-up procedures.
  - Developing media policies.

[36] French Senate (2013): *Loi de programmation militaire 2014-2019*
[37] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

- ✓ Manage the scheme: when the reporting procedures are set and running, the responsible authorities will need to pay attention to scheme management. The tasks in this stage fall into three groups:
  - Analysing and following up on individual incidents.
  - Conducting statistical analysis of a series of incidents.
  - Examining feedback to improve and evolve the scheme.
- ✓ Communicate the results of the analysis to the competent authority or authorities responsible for updating the set of minimum security measures.

> **An example: Incident reporting in Croatia**
>
> *In Croatia, Information sharing of important incidents is mandatory for systems, which are essential for proper functioning of a critical service.*
>
> *Sharing information about incidents for all other systems is voluntary. The separate sector authorities will answer the question about what an "important incident" is within their own sector.*
>
> *The different Croatian sector authorities also define the set of data that has to be shared. The general approach is to share a minimum set of data, depending on the purpose. This can be statistical data or more specific data (e.g. data shared between a CERT and the police in cases of cybercrime).*

## 4.6 Raise user awareness

Raising awareness about cyber security threats and vulnerabilities and their impact on society has become vital. Through awareness-raising, individual and corporate users can learn how to behave in the online world and protect themselves from typical risks. Awareness activities occur on an ongoing basis and use a variety of delivery methods to reach broad audiences.[38]

Security awareness activities may be triggered by different events or factors, which may be internal or external to an organisation. Major external factors could include: recent security breaches, threats and incidents, new risks, updates of security policy and/or strategy. Among the internal factors are new laws, new governments etc.[39]

Common **objectives** are to:

- ✓ Identify gaps of knowledge or awareness concerning cyber security or information security issues.
- ✓ Close the gaps by raising awareness or developing/strengthening knowledge foundations.

**Tasks** to support an awareness-raising programme include the following.[40]

- ✓ Define the target of the awareness-raising campaign (e.g. citizens, children, end-users).
- ✓ Develop mechanisms for reaching out to these communities.
- ✓ Identify common behavioural problems affecting the target audience or issues that the target audience should know about.
- ✓ Create the national information security unique identity: choose specific information security topics that support the strategy objectives and then organise and advertise, not only in Europe but also internationally, local events by using appropriate communication channels.

[38] ENISA (2010): The new user's guide: How to raise information security awareness. Available online at http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

[39] See, for instance, the proposal for a regulation 'on electronic identification and trusted services for electronic transactions in the internal market' http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

[40] ENISA (2008): Raising awareness on information security across public and private organisations.

- ✓ Organise a national cyber security month, week or day in order to engage the public, and private- and public-sector partners through events and initiatives (i.e. campaigns, workshops, conferences) with different subject matter each time.[41]
- ✓ Enhance the content of well-known governmental web sites with information security related material e.g. presentations, webinars and lectures.
- ✓ Consider translating the material into other languages.
- ✓ Support and brand European or international information security initiatives like the Safer Internet.
- ✓ Participate in relevant European initiatives and campaigns like the Safer Internet Day, International Youth Day, ENISA's security month etc.

**An example: Raising awareness by RIA in Estonia**

*RIA holds periodic events and media campaigns for raising awareness. In addition, it organises technical and end-user training. It is organising regular awareness rising and technical trainings for governmental authorities and vital service providers. In addition to trainings, RIA organises annual CIIP Seminar in every autumn.*

**An example: Action plan for raising awareness in Spain**

*According to this Line of Action 7 "Cyber Security Culture", an Action Plan has been developed to Raise the awareness of citizens, professionals and companies about the importance of cyber security. It includes a set of specific projects and actions to be developed (some of them already done or ongoing).*

*Some examples of this actions are:*

- *Under the Digital Agenda for Spain, the Spanish state has launched the Digital Trust Plan, and all of the latter's Priority 1 actions concern prevention and awareness-raising. As part of the Digital Trust Plan (DAS-5) a pilot programme is being examined which would assess the appropriateness and feasibility of incorporating a digital trust component in educational curricula.*
- *Make It Safe worldwide campaign to make the internet safer for children and adolescents.*
- *The Ministry of Interior collaborates in all institutional prevention campaigns aimed at raising awareness of cybercrime, among those sections of the population considered most at risk: senior citizens, secondary school pupils and vocational training students, and university students, via annual cybersecurity conferences and monthly talks.*
- *National Cryptologic Centre: Specific awareness campaigns and Workshops for Public Administration.*

## 4.7 Strengthen training and educational programmes

Increased investments in cyber security related education programmes as well as general education about information security threats for end user is an important pillar to decrease risks for businesses and society.[42] Unfortunately, universities and R&D institutions in many countries do not produce enough cyber security experts to meet the increasing needs of the private sector. Cyber security is usually not a separate academic topic but part of the computer science curriculum. Cyber security is also a continuously changing topic that requires constant training and education.

[41] For further information on how to organise an information security month, see ENISA (2011): European Month of Network and Information Security for All – A feasibility study. Available online at http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2011/europeansecuritymonth

[42] McKinsey Quarterly (2014): The rising strategic risks of cyberattacks. Available online at http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks

The **objectives** of a training and education program are to:

- ✓ Enhance the operational capabilities of the existing information security workforce.
- ✓ Encourage students to join and then prepare them to enter the cyber security field.
- ✓ Promote and encourage the relations between information security academic environments and the information security industry.
- ✓ Align cybersecurity training with business needs.

Typical **tasks** in this step include the following.

- ✓ Engage in dialogue with private stakeholders to determine the needs and requirements of the private sector (e.g. through surveys).
- ✓ Engage in dialogue with universities and other educational institutions to develop new programs or adapt existing one to the needs of the private sector.
- ✓ Launch national information security training and educational programmes.
- ✓ Support the security accreditation and certification of skilled personnel in key working posts in every industrial sector.
- ✓ Create a catalogue of roles, and the relevant educational background needed, with information security responsibly.
- ✓ Add information security courses to university curricula – not only to the ones related with computer science but also to any other professional speciality tailored to the needs of that profession.
- ✓ Organise information security events (e.g. hacking contest or hackathons') helping to identify national information security experts and to support networking among them.
- ✓ Create a national register with accredited cyber security experts with teaching skills.

**An example: Cyber security programmes in Estonia**

*Estonia is taking several measures to increase the number of cyber security experts in its country. The Ministry of Defence is providing grants to PhD-Students, which thesis themes related to topics in cyber security. In addition, cyber security programmes at universities have been developed, including an IT-Law-Programme at Tartu university. In order to raise awareness for information security, cyber security courses are included in all IT-related university programmes. Furthermore, secondary schools have included cyber security studies in which students can major in.*

**An example: Knowledge, skills and R&D&I in Spain**

*There are several projects on-going for this issue:*

- *Cybercamp (cybersecurity event that INCIBE organises with the aim of identifying, attracting, managing, and, in short, helping to generate cybersecurity talent that can be transferred to the private sector, in line with its demands).*
- *Network of excellence on cybersecurity R&D+i: In the context of the Trust in the Digital Domain Plan (derived from the Digital Agenda for Spain), INCIBE in cooperation with the cybersecurity research ecosystem is promoting the creation of a network of centres of excellence on cybersecurity research and innovation.*
- *Grants for advanced cybersecurity research team excellence. The initiative to launch these grants for advanced cybersecurity research team excellence has emerged to meet the current need to retain and attract cybersecurity-research talent.*
- *Different Masters in Cybersecurity delivered by Universities.*
- *Public administrations: specific training courses in cybersecurity delivered by the National Cryptologic Centre and focused for civil servants.*

## 4.8 Establish an incident response capability

National/governmental CSIRTs play a key role in coordinating incident management with the relevant stakeholders at national level. In addition, they bear responsibility for cooperation with the national/governmental teams in other countries.[43]

According to article 12 of the NIS Directive, a CSIRTs network is established with the role to contribute to the development of confidence and trust between MS and to promote swift and effective operational cooperation. Some of the tasks of the CSIRTs network include the exchange and availability on a voluntary basis of non-confidential information concerning incidents, the sharing among MS non-commercially sensitive information related to incidents, support in addressing cross border incidents on a voluntary mutual assistance basis, etc.

In order to perform their tasks properly, it is important that the national cyber security strategy empower CSIRTs with sufficient capabilities. Relating **objectives** fall within the following categories:

- ✓ Mandate – this relates to the powers, roles and responsibilities that need to be allocated to the team by the respective government.
- ✓ Service portfolio – this covers the services that a team provides to its constituency or is using for its own internal functioning.
- ✓ Operational capabilities – this concerns the technical and operational requirements a team must comply with.
- ✓ Cooperation capabilities – these encompass requirements regarding information sharing with other teams that are not covered by the previous three categories e.g. policymakers, military, regulators, (critical information infrastructure) operators, law enforcement authorities.

The following **tasks** should be considered:

- ✓ Take steps to ensure that the CSIRTs can both carry out their mandate and adhere to national and EU data-protection legislation.
- ✓ Define procedures and best practices that require CSIRTs staff to handle data in compliance with EU rules and their Member State's laws. The risks to a CERT's reputation from a data breach or misuse of personal data are too significant for a CSIRT to risk non-compliance with data protection legislation.
- ✓ Establish working groups at international or regional meetings at which CSIRTs discuss best practices and the potential of instituting common data handling protocols.
- ✓ Establish thematic working groups on data protection to involve interested stakeholders, such as the banking industry, and improve the overall information exchange.
- ✓ Consider hiring or engaging a legal expert specialising in IT security issues in order to avoid uncertainty regarding handling of personal data.
- ✓ Create a national vulnerability database and constantly assess the potential impact on critical functions or potential disturbance of core operations.
- ✓ Initiate a national project on building an early warning system for CIIs. Such systems require the cooperation of a wide range of stakeholders, both private and public, and could potentially be the central capability for handling creeping, slow-burn and sudden crises.
- ✓ Create a vulnerability disclosure framework that deals with patch and vulnerability management (period, early warning, deployment requirements, etc.). Testbeds (clones/mirrors) should be considered in order to avoid major disturbances of systems after patching essential components of critical applications.

[43] ENISA's web page on baseline capabilities for national / governmental CERTs:
http://www.enisa.europa.eu/activities/cert/support/baseline-capabilities

**An example: Community of CERTs in Poland**

*In Poland no institution is designated as the national CERT. Instead, a community of different response teams exist:*

*CERT.gov.PL is the main institution for public agencies, but also offers its services to CI operators based on formal agreements. Its tasks are to publish security notifications, to detect incidents in public networks and to resolve and analyse of incidents. It has been established in 2008.*

*The first CERT in Poland was CERT Polska, which is part of the NASK. It holds special expertise in the analysis and research of security incidents and provides information on threats and incidents. Information is available on a database that can be used by private and public entities.*

*CERT.gov.PL and CERT Polska also operate a database on honeypots. The latter response team and the IT Security Department of the Polish Internal Security Agency have developed and jointly maintain ARAKIS-GOV, an early warning system for government IT-systems.*

*In addition, there exist a number of sectoral institutions such as MilCERT and CERT Orange (telecommunications sector).*

## 4.9 Address cyber crime

The fight against cyber crime requires the collaboration of many actors and communities to be successful. In this respect, it is important to address and counter the rise of cyber crime and to prepare a concerted and coordinated response with relevant stakeholders.

Typical **objectives** to address cyber crime are:

- ✓ Creating laws in the area of cyber crime.
- ✓ Increasing the effectiveness of law enforcement agencies.

Typical **tasks** that should be considered include the following:

- ✓ Adapt the required legislation and ratify existing international treaties.
- ✓ Create specialised national cyber crime units (law enforcement and judicial authorities).
- ✓ Ensure continuous and specialised training for police and judicial authority staff (e.g. on digital forensics).
- ✓ Develop knowledge and expertise on emerging cyber crime-related threats and vulnerabilities but also attack methods through information sharing at national and international level.
- ✓ Create a harmonised set of rules for police and judicial record-keeping and appropriate tools for statistical analysis of computer crime.
- ✓ Establish forums to foster cooperation between the various players (e.g. CSIRTs and intelligence communities).
- ✓ Encourage direct action by industry against computer-related crime.
- ✓ Establish cooperation with leading academic and R&D institutions on new digital forensic techniques.
- ✓ Establish cooperation between public and private sector stakeholders to quickly identify and respond to cyber crime related issues.

For more on this topic, please check the websites of both ENISA[44] and the European Commission[45] on cyber crime.

[44] https://www.enisa.europa.eu/topics/cross-cooperation-for-csirts/law-enforcement/fight-against-cybercrime
[45] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV:l33193b

**An example: Legislation and cybercrime units in Estonia**

*Estonia has ratified the Budapest Convention and included cybercrime in the penal code (amendments were made after the 2007 large scale cyber attacks in Estonia). It includes components for cybercrime and elaborates on different types of cybercrime*

*Furthermore, Estonia has established cybercrime units in the police forces. At the regional level, designated police officers are responsible for cybercrime*

*At different social media portals, web constables (which are part of the police) are available and can be contacted to report crimes.*

## 4.10 Engage in international cooperation

Engaging in cooperation and information sharing with partners abroad is important to better understand and respond to a constantly changing threat environment.

**Objectives** related to international cooperation are:

- ✓ Benefit from creating a common knowledge base between EU Member States.
- ✓ Create synergy effects between national cyber security authorities.
- ✓ Enable and increase combating transnational crime.

The following **tasks** should be considered during the development of the strategy:

- ✓ Use the strategy as an instrument for fostering international cooperation. A strategy can indicate the Member State's stance towards international cooperation.
- ✓ Identify the countries you wish to cooperate with, explain why you want to engage with them and clarify the context of cooperation (e.g. cyber crime, operational) with each one.
- ✓ Assign to a national entity the task of promoting international cooperation. Assigning this task on a national level to a single organisation provides the benefit that all national efforts to cooperate internationally are consolidated.
- ✓ Promote international cooperation through information-sharing (for instance benchmarking, technological knowledge, and basic threat assessments), intelligence sharing, top level public–private partnerships (PPPs) (multinational), and potentially information sharing and analysis centres (ISACs).
- ✓ Join bilateral, multilateral or international treaties and conventions (e.g. International Code of Conduct for Information Security, Convention on Cyber crime) related to information security if they are compatible with the national regulatory framework and if this does not run counter to the interests of national security.
- ✓ Contribute to international efforts towards drafting standard operating procedures (SOPs) to be used for information sharing and response to real, major cross-country crises.
- ✓ Encourage participation in regional, European and international exercises as a means of supporting cooperation with strategic partners.

**An example: Denmark as a strong international partner**

*Denmark's NCSS names "Denmark as a strong international partner" as one of six focus areas.*

*There are three initiatives in this area:*

*18. Strengthening of Danish cyber diplomacy*

*19. Promotion of Denmark's stance in international cyber and information security cooperation forums*

*20. Nordic cooperation on research and education in cyber and information security*[46]

## 4.11 Establish a public-private partnership

In the majority of countries, private companies own critical infrastructure and critical services are provided by the private sector. Therefore, a high degree of communication and cooperation can be an effective way for governments to understand the needs and challenges of private companies, but also to ensure that the necessary measures are implemented to achieve a sufficient degree of security.

Public-private partnership can be an effective tool, to pool expertise and resources of the private and public sector. It establishes a common scope and objectives and uses defined roles and work methodology to achieve shared goals.[47] PPPs may focus on different aspects of security and resilience; relating **objectives** can be defined as the following:

- ✓ Deterring (to deter attackers).
- ✓ Protecting (uses research into new security threats).
- ✓ Detecting (uses information sharing to address new threats).
- ✓ Responding (to deliver the capability to cope with the initial impact of an incident).
- ✓ Recovering (to deliver the capability of repairing the final impact of an incident).

PPPs addressing security and resilience have evolved in many countries as an efficient means of protecting their critical infrastructure. Building up a successful PPP requires taking into consideration different elements as well as the challenges and barriers such structures may face.

Typical **tasks** to consider in setting up a successful PPP include the following.

- ✓ Assess the sectors in scope and the goal of the PPP; this will be a defining factor in shaping the membership and determining which external links are to be forged.
- ✓ Plan how to link the PPP with other organisations to share information and expertise and to avoid duplication.
- ✓ Assess the use of high-level strategic partnership at the CEO level in order to support senior understanding and awareness.
- ✓ Recruit real experts who are empowered from their organisations to act and change things.
- ✓ Seek legal advice to ensure that the legal framework used is suitable for the jurisdiction in which the PPP operates.
- ✓ Adopt information distribution policies such as the Traffic Light Protocol to give the source confidence that the information will be used only as agreed.
- ✓ Prepare together with a legal advisor a sample non-disclosure agreement (NDA) that describes the terms and conditions of the membership. Use this agreement and ask the parties involved to sign it.
- ✓ Make sure that all members of the partnership actively contribute in providing information, services and support that are of relevant value to the membership.
- ✓ Look for opportunities to create international links with other PPPs for cross-border sharing and collaboration.

[46] Center for Cyber Security (2015): The Danish Cyber and Information Security Strategy. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-strategy-for-cyber-and-information-security/at_download/file

[47] ENISA (2011): Cooperative Models for Effective Public Private Partnership - Good Practice Guide. Available online at https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps/at_download/fullReport

**An example: Austrian Cyber Security Platform**

*The Austrian Cyber Security Platform shall be established as a public private partnership to facilitate ongoing communication with all stakeholders of the administration, economy and academia. In parallel, existing initiatives (e.g. Austrian Trust Circle, Cyber Security Austria, Kuratorium sicheres Österreich, A-SIT8, …) will be carried on and taken advantage of. The Austrian Cyber Security Platform will provide the institutional framework for a permanent exchange of information within the public administration as well as between the public administration and representatives of the economy, science and research. All stakeholders will participate on an equal footing. The Cyber Security Platform advises and supports the Cyber Security Steering Group.*[48]

**An example: Private sector cooperation in Bulgaria**

*Public-Private Partnership - Improving Cyber-security requires a combined, multi-sector, comprehensive approach that focuses on building a "whole-of-government" cyber organisation that includes cooperation with private enterprises and places an emphasis on educating the citizen. Opportunities to enhance the involvement of the private sector and to ensure that we capitalize on their expertise should include jointly exploring best practices and procedures to ensure that no part of the critical infrastructure, whether in public or private hands, would become a weak link and vulnerability.*

**An example: Planned PPP for cyber security in Belgium**

*The development of a PPP is one of the mission targets of the CCB. It shall act as an Information Sharing and Analysis Centres (ISAC), with the following tasks:*

- *fostering of partnerships*
- *fostering of information sharing*
- *sharing of expertise and knowledge*

## 4.12 Balance security with privacy and data protection

A cyber security strategy should seek for the right balance between these two concepts. Moreover, the European Commission has provided the regulatory tools to support the Member States in facing this challenge. For this reason, every Member State should take seriously into account the right of citizens' privacy. Finally, privacy is a horizontal issue that cuts across most of the activities relevant to cyber security strategy.

The main **objective** is to:

- ✓ Find a balance between security needs and privacy and data protection rights of citizens.

Typical **tasks** to consider include the following.

- ✓ Take into account national legal requirements for data protection when drafting cyber security relevant regulatory texts.
- ✓ Take the advice of the data protection authority(ies) on regulatory texts related to cyber security.
- ✓ Consider data protection law compliance measures when consulting the minimum security measures.
- ✓ Make data protection supervisory authority(ies) part of information security compliance audits to the most critical stakeholders.

[48] Bundeskanzleramt Österreich (2013): Austrian Cyber Security Strategy. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/austrian-cyber-security-strategy

- ✓ Support and brand, together with the national data protection authority(ies), the European Data Protection Day (January 28).
- ✓ Involve national data protection authority(ies) in national cyber exercises, if the scenario is relevant to data protection issues.

**An example: Finish Data Protection Ombudsman and FICORA**

*The Data Protection Ombudsman: guides and controls the processing of personal data and provides related consultation. The Ombudsman exerts power in issues related to the implementation of the right of verification and the correction of personal data. The Ombudsman also follows the general development in the processing of personal data, launching initiatives if necessary. The Ombudsman sees to the distribution of information related to the field of operation and participates in international co-operation.*

*The Finnish Communications regulatory Authority (FICORA) supervises the data protection of electronic communications in the operations of telecommunications operators, corporate or association subscribers, and in other communications providers' operations. FICORA supervises, for example, processing of identification data, protection of communications and decoding, and compliance with the provisions on the information service of communications services.*

*FICORA is the competent national authority referred to in article 2 of the Commission Regulation 611/2013 hence It receives telecommunications operators' notifications of personal data breaches. Information collected through these notifications is used in directing FICORA's steering and supervision of telecom operators.*

*The Data Protection Ombudsman and FICORA collaborate with each other regularly and if needed, also case by case.*

**An example: The Slovenian Government Office for the Protection of Classified Information**

*In the field of cyber security The Government Office for the Protection of Classified Information will assume the role of the National Cyber Security Authority. It will become a coordinating body in the strategic level of the national cyber security system and a National point of contact for international cooperation.*

## 4.13 Institutionalise cooperation between public agencies

Cyber security is a problem area that spans across different sectors and across the responsibilities of different public agencies. Therefore, close cooperation between these entities is an important pillar for the successful implementation of NCSS.

The institutional setting for an institutionalised form of cooperation can range from advisory boards, steering groups, forums, councils, cyber centres or expert meeting groups. In addition, the purpose of the institution can vary between consultation, sharing information or the coordination of actions between the different agencies. In order to set up an institution for coordination, governments either can develop new kinds of cooperation mechanisms for the specific purpose of cyber security or extend the scope of existing institutions.

The main **objectives** are:

- ✓ Increase the cooperation between public agencies with responsibilities and competencies related to cyber security.
- ✓ Avoid an overlap of competencies and of resources between public agencies.
- ✓ Improve and institutionalise cooperation between public agencies in different areas of cyber security.

Typical **tasks** to consider in this step include the following.

- ✓ Determine the purpose of the new institution (e.g. risk assessment, CERT-cooperation, information-sharing about vulnerabilities, advisory).
- ✓ Determine the relevant public agencies, which are needed to fulfil the purpose of the new cooperation body.
- ✓ Define the tasks and responsibilities of the new cooperation form.
- ✓ Determine and establish the type of institutionalised cooperation between the public agencies, e.g.:
  - Committee
  - Working, steering or meetings group
  - Forum
  - Councils
  - Advisory boards
- ✓ Define the kind of participants and representatives of the different agencies to attend the meeting.
- ✓ Define the agenda and topics to be discussed.
- ✓ Describe the role, responsibilities and tasks of the new institution in the NCSS.

**An example: The Swedish Cooperation Group for Information Security (SAMFI)**

*In order to coordinate the actions between the different agencies and public entities, the Swedish government has developed a cooperative network comprised of authorities "with specific societal information security responsibilities". This Cooperation Group for Information Security (SAMFI) consists of representatives of the different authorities and meets several times a year to discuss issues related to national information security. SAMFI's subject areas are mainly to be found in political-strategic areas and cover topics such as technical issues and standardization, national and international development in the field of information security, or management and prevention of IT incidents.*[49]

**An example: The German National Cyber Security Council and the National Cyber Response Centre**

*The National Cyber Security Council has been established pursuant to the German Cyber Security Strategy (GCSS). It is comprised of representatives from relevant ministries and public agencies as well as selected business representatives. The council meets three times a year and has the goal of discussing and coordinating actions between the different stakeholders on a political-strategic level.*

*The National Cyber Response Centre has been established in accordance to the GCSS between April 2011 and March 2013. Here, representatives from the different relevant public authorities and law enforcement agencies come together to share information and to assess cyber security incidents from different perspectives.*[50]

## 4.14 Foster R&D in cyber security

Research and development in cyber security is needed in order to develop new tools for deterring, protecting, detecting, and adapting to and against new kinds of cyber attacks.

Typical **objectives** of this phase include the following.

- ✓ Identify the real causes of the vulnerabilities instead of repairing their impact.

[49] ENISA (2016): Stocktaking, Analysis and Recommendations on the protection of CIIs. Available online at https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

[50] ENISA (2016): Stocktaking, Analysis and Recommendations on the protection of CIIs – Annex. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex

- ✓ Bring together scientists from different disciplines to provide solutions to multidimensional and complex problems such as physical-cyber threats.
- ✓ Bring together the needs of industry and the findings of research, thus facilitating the transition from theory to practice.
- ✓ Find ways not only to maintain but also to increase the level of the public's trust in existing cyber infrastructure.

Typical **tasks** in this step comprise the following.

- ✓ Create a forum for industry and request R&D topics for consideration.
- ✓ Create an R&D agenda with topics that support the objectives of the cyber security strategy with a midterm horizon, of between four and seven years. For each topic the following should, at least, be described: the objective, the incentives and the challenges of the topic.
- ✓ Create research funds, which support research programmes in the area of cyber security.
- ✓ Create a platform for bringing together high-level research and the private sector. This platform may take the form of a public–private partnership.
- ✓ Seek cooperation with similar European and international relevant activities i.e. the European Commission Research and Innovation programmes (e.g. FP7/8, H2020).
- ✓ Create a coordination research plan in order to avoid overlaps between research activities undertaken by different institutions and programmes.
- ✓ Develop effective incentives to make cyber security research ubiquitous. Both individuals and organisations might be the beneficiary of these incentives.

**An example: The Swedish framework programme on information security 2011-2016**

*The framework-programme on information security 2011-2016 is themed on organization's ability to create a culture of security that involves a high security awareness among management and employees.*

*The Swedish Government funds different research programmes (some of them through the Swedish Civil Contingencies Agency). There is currently a 4-year programme running, involving 3 million Euro, which are provided to different research activities. Furthermore, the government is cooperating with the Royal Institute of Technology regarding a 5-year programme in the area of SCADA/ICS systems. In addition, Sweden is cooperating with the USA for R&D.*

## 4.15 Provide incentives for the private sector to invest in security measures

There are different ways how governments can ensure that businesses implement appropriate security measures. One way is to make certain standards mandatory by law. However, governments can also apply softer steering measure, for example by giving incentives to businesses to invest in certain security measures.

Typical **objectives** are:

- ✓ Identify possible incentives for private companies to invest in security measures.
- ✓ Provide companies with incentives to encourage security investments.

Typical **tasks** to consider in this step include the following.

- ✓ Examine if positive incentives can be provided to operators of CII to invest in security measures.
- ✓ Encourage companies to invest in security measures through "soft" steering tools, such as tax breaks or financial subsidies.
- ✓ Support R&D by setting up research programs or funds.

- ✓ Support companies with post-incident management. Develop capabilities to help operators with forensic investigations and recovery measures.

**An example: Incentives for the private sector to invest in security measures in Finland**

*In order to ensure cyber security development, Finland will see to it that appropriate legislation and incentives exist to support the business activities and their development in this field. Basic know-how in the field is gained through business activity.*[51] *For example, a key project of the Government is the creation of a growth environment for digital business operations in Finland. One of the principal measures under this key project is the preparation and implementation of a national information security strategy for increasing the level of trust in the Internet and in digital practices. The strategy was prepared in close cooperation with private sector. A development group for information security in business was set up to support the preparation of the strategy.*

*The strategy is intended to focus on ensuring competitiveness and the right conditions for exports, developing the EU's digital single market and safeguarding privacy protection and other fundamental rights. The strategy aims to bring about change whereby information security will be an integral part of different systems, terminal devices and services. The strategy also deals with matters that damage trust, such as information security violations and large-scale infringements of privacy protection in networks.*

[51] Secretariat of the Security and Defence Committee (2013): Finland's Cyber security Strategy. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

# 5. Identified challenges

Based on the desk research and interviews, this chapter presents challenges and obstacles that countries were facing during the development and implementation of their NCSS.

### Establish effective cooperation between public stakeholders

Establishing effective cooperation between stakeholders was named by many countries as one of the major challenges they were facing during the implementation of their NCSS. Cooperation in the area of cyber security is new for some public stakeholders in many cases and requires a change of habits. A major challenge for cooperation are different interests and competencies between the relevant public stakeholders. In addition, the problem is often caused or compounded by the lack of a clear governance structure.

By nature, cyber security and cyber incidents span across different areas and different areas of responsibilities.

Related to this issue is the problem of mainstreaming dialogue and vocabulary regarding digital risk management and digital security governance across both the public sector.

### Establish trust between public and private stakeholders

Many countries have named trust issues between public and private stakeholders as one of the main obstacles in the implementation of core objectives, such as establishing baseline and security requirements, incident reporting or establishing public private partnerships. The establishment of trust is a process, which requires extensive dialogue as well as time and effort. Companies are reluctant to report security incidents, because of potential loss of reputation. Trust issues are especially apparent in cases where authorities were given a strong mandate with certain powers and authorities or new laws were planned which would obligate private stakeholders to implement certain security measures.

In addition to general trust issues, cultural factors can add to the problem. In countries with liberal market policies and a negative perception of security issues, this can lead to a reluctance of stakeholders to take advice from professional bodies. This can lead to a vicious circle: If no obligation to report incidents exists, than there will be no awareness about the current cyber threat situation. Because of the lack of knowledge, no actions are taken to increase cyber security.

### Ensure adequate of resources

An important obstacle in the implementation of NCSS can be a lack of resources. Some of the cyber security public authorities named the lack of funding and financial resources as a problem for the execution of measures. Resource-intensive objectives, for example the development of cryptographic algorithms, require adequate financial and personal resources. In addition, some public agencies named a general lack of skilled personal as a main challenge.

### Promote a common approach and awareness for privacy and data protection

The lack of a common approach for security in general and privacy in particular was named as a major obstacle by countries, which NCSS is focused around business and growth for digital business. Furthermore, the lack of a joint approach regarding the flow of data inside the EU and towards the situation of the confidentiality of communication of citizens and business is perceived as a hurdle.

Furthermore, gaining awareness for information security proved difficult in countries, in which the public perceives security as intrusive surveillance and an unwanted intrusion on personal rights and liberties. This can lead to a lack

of understanding of the cross-cutting nature of digital services and of pervasiveness of cyber security and insufficient cooperation and coordination between national data protection authorities and information security authorities.

### The implementation of vulnerability and risk analysis

The implementation of vulnerability and risk analysis was challenging for certain countries, because in the beginning the focus was set too broad and the approach was focusing on an integral risk management, which proved to be too challenging as well as resource and finance intensive. The scope of risk analysis needs to be chosen carefully; otherwise, the design can be too comprehensive and cover too many risk areas. This can result in too capital and resource intensive measures.

# 6. Evaluate the national cyber security strategy

Once the strategy has been developed and is being executed, the extent to which the objectives are achieved should be assessed. By assessing the achieved results of the activities, it is possible to take any required corrective and preventative actions that will lead to the next strategy.

This chapter will cover the explicit requirements needed to evaluate and adjust the strategy. Evaluation is necessary to determine whether the objectives and the planned results have been effectively reached. The primary purpose of evaluation, in addition to gaining insights into the status of the existing initiatives, is to identify future objectives of the next strategy.

## 6.1 Evaluation approach

There are different methodologies to evaluate a strategy. In this chapter, we will not propose a specific one but rather focus on specific, practical actions necessary to perform an evaluation. This process should end with a report on the status of affairs and a list of actions that the national cyber security strategy owner(s) should implement.

The following suggestions can be considered in defining the strategy evaluation report.

- ✓ Define the scope of the evaluation, the key objectives, the expected outcomes and the periodicity of it.
- ✓ Implement the 'Segregation of duties' principle: assign to an independent entity, a supervisor or a trusted third party (other than the national cyber council) the task of evaluating the effectiveness of a national cyber security strategy and its activities (e.g. a national cyber security council).
- ✓ Empower the independent entity with the appropriate mandate, role and responsibilities to succeed in this operation.
- ✓ Encourage and offer incentives to stakeholders to be involved in the evaluation process.
- ✓ Evaluate not only the strategy but also the individual tasks of it.
- ✓ Follow both a quantitative and qualitative approach giving emphasis on both impact and results.
- ✓ Perform an internal/self-impact assessment for each activity of the strategy taking into consideration the opinion of the stakeholders.
- ✓ Perform an external impact assessment for each activity of the strategy taking into consideration the opinion of external and/or affected users/communities.
- ✓ Evaluate each activity against the action plan and key performance indicators (KPIs) agreed when the activity kicked off; evaluate KPIs through questionnaires (online) and polls within the stakeholder community.
- ✓ Create a data collection scheme for obtaining relevant data for the evaluation of the strategy and the action plan. Effectiveness of the strategy should be measured at all levels. The data collection process should become comprehensive.
- ✓ Identify lessons, good practices and bad practices from the internal and external impact assessment as well as the evaluation of each activity.
- ✓ Prepare an analytical evaluation report describing the achieved results and the expectations for the next evaluation.
- ✓ Carry out benchmarking studies in order to compare strategies between different Member States. The outcomes of a benchmarking study can be used to identify areas of improvement.

## 6.2 Key performance indicators

This chapter presents a list of possible and indicative KPIs for the key strategic objectives presented in chapter 4. These allow policy-makers to track the success of the implementation of strategic objectives. With regard to the presented quantitative measures, it needs to be mentioned, that these KPIs alone are not sufficient to measure successful implementation. Both quantitative and qualitative KPIs should be used in evaluation.

- ✓ **Develop national cyber contingency plans:** An NCP aims to develop a national response capability and promote overall coordination among the hierarchy of emergency response organizations and response or contingency plans. Typical KPIs include:
  - The number of activities of a national cyber contingency plan that have been completed on time.
  - The number of sectors and stakeholders involved in the development of the plan.
  - The number of national cyber exercises to test the plan.
  - The number of sectors and stakeholders involved in the development of the plan.
  - The level of preparedness to respond to a cyber crisis based on different scenarios (potential causes and different levels of impact).
  - The existence of crisis management facilities and situation rooms.
- ✓ **Protect critical information infrastructure:** Comprehensive protection of critical information infrastructure necessitates the inclusion of all relevant sectors as well as providers of CII. Typical KPIs include:
  - The existence of a method for the identification of CIIs.
  - The comprehensiveness of the identified critical sectors.
  - The comprehensiveness of the identified providers of CII.
  - The involvement of relevant private, public and civil stakeholders.
  - The comprehensiveness of the identified risks per critical sector.
  - The existence of a national risk registry for identified or known risks.
  - The comprehensiveness of security policies per critical sector.
  - The number of implemented security measures per critical sector (to measure the performance of security measures see KPI's for "Establish baseline security measures".
- ✓ **Organise cyber security exercises:** Exercises are an important tool to assess the preparedness of a community for natural disasters, technology failures and emergencies. For this reason, it is important to develop specific metrics to gauge the success of the exercises. Typical KPIs include:
  - The number of cyber security exercises conducted.
  - The status of actions implemented based on the findings/evaluation reports.
  - The number of sectors involved.
  - The number of people involved.
  - The level of involvement of the private sector.
  - The number of plans and procedures that have been tested.
- ✓ **Establish baseline security measures:** Baseline security measures are the result of a consultation process between the relevant national cyber security stakeholders. It is expected that competent authorities will monitor the implementation of these measures on a regular basis. Typical KPIs include:
  - The number of incidents; individual indexes of this kind might be:
    - The number of incidents that failed to be addressed by the measures.
    - The number of incidents that are addressed by the measures.
  - The number of non-compliant organisations identified within a specific period of time.
- ✓ **Establish incident reporting mechanisms:** Receiving, collecting and analysing data about incidents is important not only to initiate short-term mitigation measures, but also to gain situational awareness and knowledge about the current threat environment. Typical KPIs include:
  - The number of incident reports received.
  - The number of sectors that participate in the reporting scheme.
  - The number of stakeholders that participate in the reporting scheme.

- The number of cyber security landscape reports or other kinds of analysis prepared by the entity that receives the incident reports.

✓ **Raise user awareness:** Indicators for the performance of user awareness measures are the number of campaigns and similar events arranged by public and private entities. These measures should focus on areas, in which a lack of awareness or knowledge has been identified.
- The existence of measures to identify target areas for awareness raising.
- The areas/topics covered by awareness raising campaigns (e.g. end-user, children, CIIP).
- The number of public awareness raising events (e.g. conferences, workshops).
- The number of corporate in-house awareness raising measures.

✓ **Foster R&D:** In order to foster research and development, governments need to support and invest in research programmes at universities or develop public research projects. Typical KPIs include:
- The relative size of budgets allocated to cyber security research per year.
- The number of cooperation agreements with universities and other research facilities.

✓ **Strengthen training and educational programmes:** Education about information security as well as skilled personnel in key position is imperative to increase the overall level of national cyber security. Typical KPIs include:
- The number of cyber security courses established.
- The number of annual information security events (e.g. hacking contests or hackathons).
- The number of accredited or certified personnel in the private and public sector.

✓ **Establish an incident response capability:** In order to mitigate incidents it is important to develop a comprehensive network of national CSIRTs, which cooperate with each other, share responsibilities as well as information. Typical KPIs include:
- The number of sectorial and national CSIRTs established.
- The number of entries in the national vulnerability database.
- The number of annual meetings or workshops between national CSIRTs.
- The number of cooperation with foreign CSIRTs.

✓ **Address cyber crime:** Allocated budgets to cyber crime units and other law enforcement authorities are an important indicator of the importance of cyber security in a country. Typical KPIs include:
- The existence of cyber crime units.
- Allocated budgets to cyber crime units.
- The number of cyber crime personnel in law enforcement authorities.
- Cyber crime reports:
  - The number of cyber crimes conducted.
  - The number of convicted cyber criminals.

✓ **Engage in international cooperation:** International cooperation can be established across different areas and potentially expands across several of the objectives described in this guide. Therefore, the focus here will be on general KPIs:
- The number of cooperation agreements with other countries.
- The number of signed or ratified international treaties or conventions in the area of cyber security.
- The number of national public agencies in the area of cyber security that are involved in international cooperation schemes.
- The scope and amount of information exchange between national cyber security authorities.
- The number of international cyber security exercises.
- The number of international stakeholders involved in international cyber security exercises.

✓ **Establish a public-private partnership:** Public-private partnerships can be an effective tool for increased cooperation between public and private actors. Typical KPIs include:
- The number of established public-private partnerships.
- The range of issues areas covered by existing public-private partnerships.
- The number of public and private stakeholders involved in public-private partnerships.

- ✓ **Balance security with privacy:** When implementing cyber security measures, data protection should be taken into account adequately. A typical KPI is the existence and involvement of a national data protection authority. Therefore, typical KPIs are:
  - The existing of a national data protection authority.
  - The existence and comprehensiveness of national data protection laws.
  - The degree of involvement of the national data protection authority in cyber security related issue areas (e.g. drafting new laws and regulations, defined minimum security measures).
- ✓ **Institutionalise cooperation between public agencies:** Indicative KPIs for the performance of institutionalised cooperation schemes are the number of participating stakeholders and tasks and responsibilities of these cooperation platforms.
  - The number of relevant public authorities involved or participating in the cooperation scheme.
  - The number of institutionalised forms of cooperation (e.g. committees, working groups, forms, councils, advisory boards).
  - The scope of cooperation platforms (e.g. tasks and responsibilities, number of issue areas).
  - The number of annual meetings.
- ✓ **Provide incentives for the private sector to invest in security measures:** To measure if incentives are working, it should be measured if these lead to stronger investments in security measures by private actors.
  - The budget available to provide incentives for the private sector.
  - The number of private actors that react to incentives by investing in security measures.
  - The number of additional security measures implemented by actors that make use of incentives.

## 6.3 Status of implementation and identified gaps

Based on the analysis of 22 EU Member States and EFTA countries, this section will describe which areas (objectives) are the best and the least developed. For this purpose, we examined the status of the implementation of the 15 objectives described in chapter 4. The status of the implementation has been divided into three categories:

- Low degree of implementation: <10 countries have largely implemented the objective
- Medium degree of implementation: between 10 and 16 countries have largely implemented the objective
- High degree of implementation: >16 countries have largely implemented the objective

### 6.3.1 Low degree of implementation

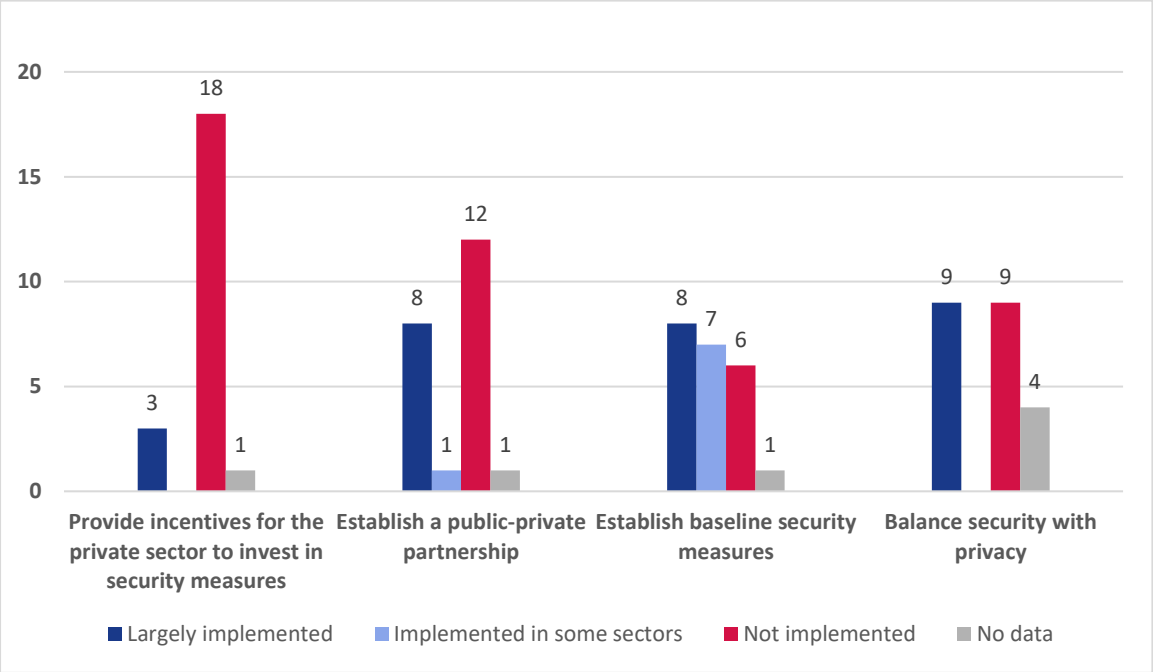


**Figure 6-1 – Low degree of implementation**

Providing **incentives**, especially monetary incentives, to private companies in order to encourage them to invest in security measures is not a tool favoured by the vast majority of the examined countries. Only three countries are offering incentives of various kinds. These include **tax breaks** and **VAT exemptions** for investments in cyber security R&D. Eighteen countries have not implemented any financial incentives for the private sector. Some of these countries consider information security solely as **market question** and as a **competitive factor** in the business for digital products and services.

Public-private partnerships (PPPs) are considered an **effective tool to ensure close cooperation between public and private stakeholders** across different issue areas. However, only a minority of twelve countries have yet established public-private partnerships for the purpose of cyber security.

Only eight countries have established baseline security requirements across all sectors. These requirements vary between **organisational and technical measures, security audits and mandatory incident reporting**. However, seven countries have established such requirements only for specific sectors. The telecommunication, energy and banking sectors remain the most regulated ones. Six countries have not established any baseline security requirements. This is because they are still at an early stage of implementation, or because of liberal market policies.

Privacy is a topic, which has gained momentum in recent years through events such as the global surveillance disclosures or the recent legal dispute between Apple and Federal Bureau of Investigation (FBI) on phone encryption. To determine if countries appropriately consider the **balance between security and privacy**, we examined if and to what extent the national **data protection authority (DPA)** is involved in the development of strategy papers, measures and preparation and drafting of legal documents. In nine countries, the DPA works together with the respective cyber security authorities in at least one of the mentioned areas (to varying degrees). In nine countries, the national DPA is not formally involved in these issues.

### 6.3.2 Medium degree of implementation

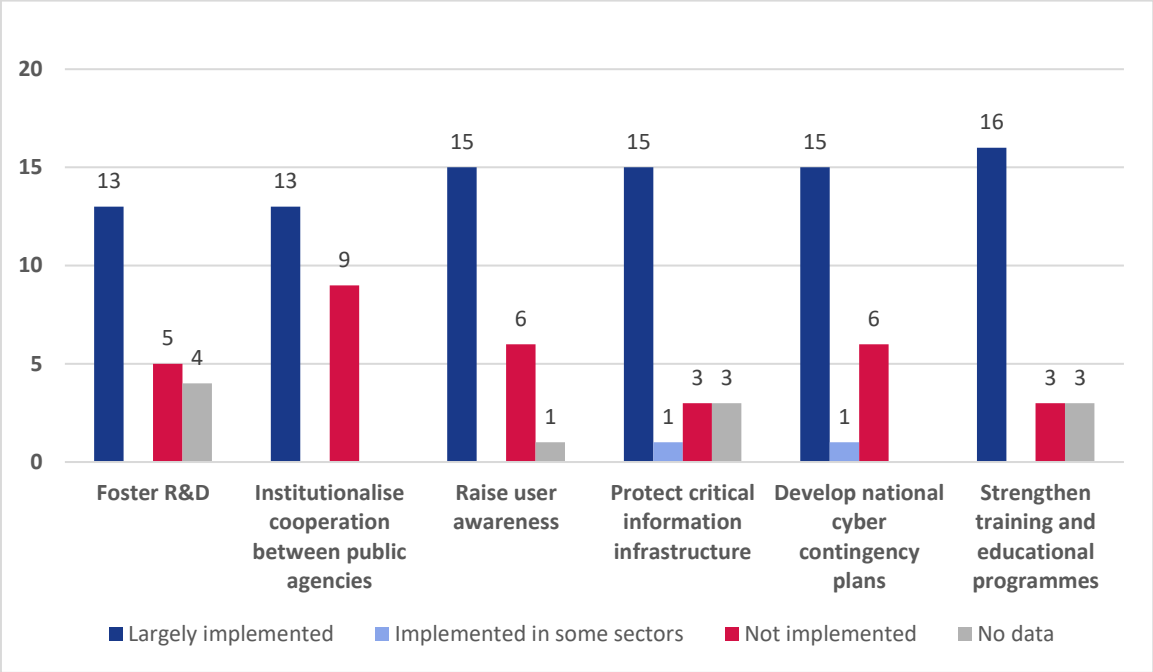


**Figure 6-2 – Medium degree of implementation**

The measures with regard to research and development in cybersecurity are very different across the examined countries. Fostering R&D in most cases is done by creating **public research funds or through collaboration with academic institutions**. Some countries have created R&D divisions within their public agencies responsible for cyber security.

The establishment of institutionalised forms of cooperation between public agencies for the purpose of cybersecurity is handled differently across the examined countries. Thirteen countries have created **cooperation groups, committees, working groups, interministerial positions or similar institutions** for this purpose. Nine countries trust in conventional or informal communication channels.

Fifteen countries have established some type of user awareness measure in their country. User awareness measures take very different forms and range from **awareness campaigns at schools** to **seminars for employees of operators of critical infrastructure** organised by CSIRTs. Six countries have yet to develop and implement user awareness measures.

To determine, if countries are determined to **protect critical information infrastructure**, we examined if countries have **developed and applied a method for the identification of providers of critical infrastructure** in their country. Fifteen countries have identified the operators or providers of critical infrastructure in their country. One country is currently in the process of identification.

In order to establish whether countries have **developed national cyber contingency plans**, we examined whether or not **roles and responsibilities in case of a cyber emergency** have been defined and documented. Fifteen countries have developed such governance structures, while six countries lack defined responsibilities. Most countries have embedded responsibilities for cyber emergencies in their overall national crisis or emergency management structures. The six countries that are lacking cyber contingency plans are still at an early stage of implementation of their NCSS or have yet to develop one.

The examined countries have developed different measures to **strengthen training and educational programmes**. Some countries are engaged in **intensified dialogue with private stakeholders and academic institutions**. The goal is to develop new cyber security courses at universities or to include cyber security in existing ones. Other governments are offering **cyber security trainings for civil servants**. Sixteen of the examined countries have implemented such measures to increase the number of cyber security experts in their country.

### 6.3.3 High degree of implementation

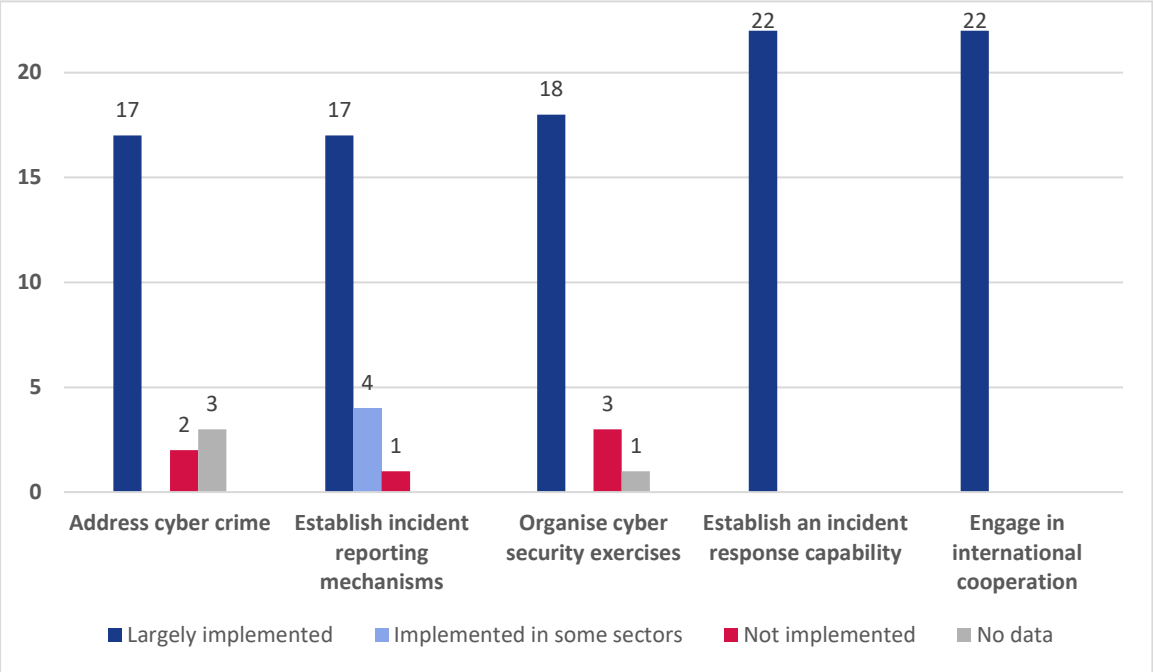


**Figure 6-3 – High degree of implementation**

Seventeen countries have addressed cybercrime. This was achieved through **new legislation, the allocation of dedicated resources** to law enforcement agencies or the developed or **new cyber crime units**.

For objective #10 "Establish incident reporting mechanisms", we examined if countries have **designated a public agency to which companies or public entities can report security incidents** and if the necessary processes for incident reporting are defined. Seventeen countries have tasked agencies with this function. The type of agency varies between countries, but the task is usually assign to the main cyber security authority or a national CERT. Four countries have established sector-specific reporting mechanisms. In these cases, the task usually assigned to a sector-specific regulator.

Eighteen countries have **conducted national cyber security exercises** in the past. However, some countries **limit those exercises to core sectors**, while others are conducting exercises with stakeholders across all critical sectors. This is partially due to different definitions of "critical sectors", but also because of different levels of sophistication of the sector-specific authorities or the relationship between regulators and providers of critical infrastructures. In some cases, cyber exercises are not stand-alone but **integrated into overall national crisis exercises**.

All of the twenty-two examined states have implemented objective #9 "Establish an incident response capability". All of the countries have established some kind of incident response capability in the form of a **National CERT, GovCERT or sector-specific CSIRTs**. In most countries multiple CERTs or CSIRTs exist, which are responsible for different entities and often complement each other in their respective tasks.

In addition, all of the examined countries were in involved in some kind of international cooperation. Most countries participate regularly in ENISA's exercise **Cyber Europe or NATO's cyber exercise Locked Shields**. Some of the examined countries are participating in exercises with a more regional focus, for example **CyberEx or Baltic Cyber Shield**. Participation in international exercises is the strongest part of international cooperation. However, some states are also engaged in information sharing and cooperation between foreign law enforcement agencies or in joint research programs.

## 6.4 Mapping exercise

The following map is the result of the mapping exercise. It displays the status of implementation of national cyber security strategies in EU Member States and EFTA countries. For this we analysed, which of the 15 objectives described in chapter four have been put into action by the individual countries. If a country has at least fulfilled one of the subtasks of an objective, an icon for that objective is displayed.

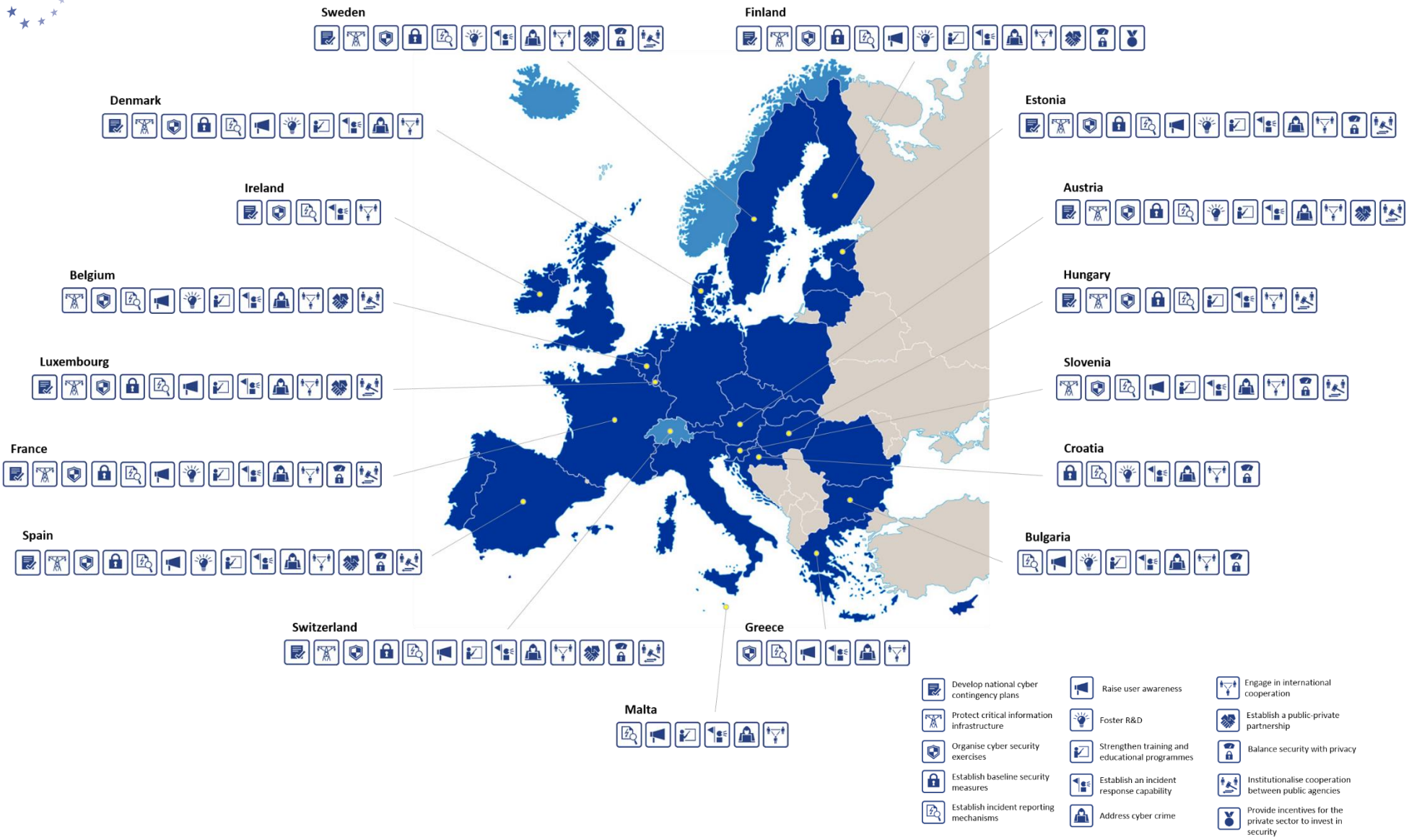


**Figure 6-4 – Mapping exercise**

# 7. Recommendations

Based on the identified challenges and gaps, good practices and the requirements of the recently published NIS Directive, ENISA presents the following recommendations for EU Member States.

### Recommendation 1: Consider to include the provisions of the NIS Directive into the NCSS

The European Parliament adopted the Network and Information Security Directive in July 2016 and one of its objectives is to improve EU Member States' national cybersecurity capabilities. For this purpose, EU Member States are required to develop and adopt a NCSS and implement several additional measures. In particular, the NIS Directive requires states to:

- Develop and adopt a NCSS, including a risk assessment plan, measures relating to preparedness, response and recovery, indication of awareness-raising and training programmes, and an indication of research and development plans (Article 7).
- Designate one or more national competent authorities for the purpose of the security of information systems, which shall act as a single point of contact (Article 8) and provide the authorities with the necessary powers and means (Article 17).
- Designate one or more CSIRTs (Article 9).
- Ensure that either the national competent authority or the CSIRT receive incident notifications (Article 10).
- Identify operators of essential services for critical sectors (Article 5) and provide indication of their relative importance.
- Ensure adequate cooperation at the national level (Article 10).
- Develop security requirements for operators of essential services and establish incident notification (Article 14).
- Lay down rules for effective, proportionate and dissuasive penalties (Article 21).

If needed, Member States can call upon ENISA to assists them in drafting a NCSS and developing measures. Implementing the NIS Directive will require EU Member States to adapt their NCSS, draft appropriate laws and regulation and develop frameworks and corresponding capabilities.

### Recommendation 2: Consider prioritizing certain critical sectors

The NIS Directive names seven critical sectors, which EU Member States should consider when planning and implementing cyber security measures. We recommend that EU Member States, which are in an early stage of development or implementation of their NCSS, should consider whether certain sectors could be prioritized. Reasons to prioritize certain sectors are an already high degree of awareness for cyber security or available resources. A focused approach rather than a "cover everything" approach can provide several advantages: EU Member States can make fast progress by rolling out cyber security measures in sectors, which are already in an advantageous position. These sectors can provide a positive example, when approaching stakeholders of other critical sectors at a later stage.

### Recommendation 3: Align or integrate CIIP with NCSS and national emergency management structures

Critical information infrastructure protection is an integral part of a NCSS. With regard to incident and emergency response, there is also a conceptual and often organizational overlap between CIIP and existing national emergency management structures.

We recommend aligning CIIP with the national cyber security strategy and the national emergency management structures to avoid ambiguities relating to lines of responsibilities, duplication of structures and measures, and waste

of resources. Roles and responsibilities of public agencies and private entities in case of cyber security incidents should be clearly defined.

Responsibilities for cyber security related incidents are often separated from the overall national emergency management structures. In these cases, a clear definition of cyber security incidents is needed. Alternatively, responsibilities can be embedded and aligned with existing national emergency structures. For this, cooperation and information sharing mechanisms between the national cyber security authority and the national emergency management authority have to be developed. The same applies to roles and responsibilities with respect to risk assessment methods and the development of national contingency plans.

### Recommendation 4: Extend the scope of international cooperation beyond international exercises

Currently, international cooperation between EU Member States is mostly limited to joint cyber security exercises. International cooperation in other areas, such as sharing of threat information, early warning systems, research and development, or training and education programmes are less developed. However, since cyber crime is a transnational problem, member states can highly benefit from cooperation in these areas. In addition, multinational corporations can benefit from standardized baseline requirements across the European Union. Therefore, it is recommended to extend the scope of international cooperation beyond cyber security exercises.

The need of an extended scope of international cooperation is also reflected in article 11, 12 and 13 of the NIS Directive, which calls for the establishment of an EU-wide cooperation group and closer cooperation between national CSIRTs.

### Recommendation 5: Create a common understanding of concepts and terminology

A lack of cooperation between public sector agencies and between the public and the private sector has been named as one of the major obstacles for effective implementation of NCSS. One of the main barriers for cooperation between the different entities are different understandings of concepts and definitions with regard to cyber security. Therefore, it is recommended to reach a mutual understanding of concepts and create a common terminology across public and private sector entities.

This recommendation is also reflected in article 3 of the NIS Directive, which calls for a minimum degree of harmonization and provides a set of definitions for cyber security related terms for this purpose.

### Recommendation 6: Approach and involve stakeholders at an early stage of development

Certain EU Member States were successful in increasing the willingness of private actors for future collaboration by approaching them at an early stage of development of their NCSS, new laws or measures.[52] When drafting new legislation or developing a new or updated NCSS, it is recommended to engage private stakeholders at an early stage of the process.

- Thereby, stakeholders have the possibility to voice concerns, which can be taken into consideration by public cyber security agencies. If concerns of the private stakeholders are taken into account, stronger commitment to the results can be expected. A good starting point to engage private stakeholders is through institutionalized cooperation mechanisms, e.g. through PPPs. However, many EU Member States are still lacking such cooperation platforms (see  High degree of implementation: >16 countries have largely implemented the objective

Low degree of implementation).

[52] ENISA, KPMG (2016): Interview questionnaire Austria; ENISA, KPMG (2016): Interview questionnaire Malta.

### Recommendation 7: Gain situational awareness

Situational awareness with regard to cyber security includes knowledge about the current threat situation, activities of relevant public agencies and the overall status of the implementation of measures with regard to the NCSS. In order to gain a comprehensive overview of the national cyber security situation, close collaboration and input is needed from relevant public agencies, such as cyber security agencies, law enforcement units, CSIRTs, ministry of interior, ministry of defence and sector-specific regulatory authorities.

A risk analysis approach should be developed and implemented by a designated authority (see Step #2 Follow a risk assessment approach). The results of such analysis help to gain a holistic understanding of current threats and risks. Risk analysis can be conducted for the country as a whole, or in relation to specific critical sectors.

The input of different agencies and the results of the risk analysis can be aggregated in a regular report, which can be made available to operators of critical infrastructures. In order to gain an overview of the implementation of NCSS measures, a roadmap should be defined, which outlines the overall agenda. Defined KPIs can be used to track the overall progress of the different measures.

### Recommendation 8: Develop requirements and measures per critical sector

EU Member States need to ensure that operators of critical infrastructure and provider of essential services take necessary measures to secure their information systems in appropriate manners. Member States can guide the efforts of the private sector by developing generic requirements and measures for critical sectors. Generic requirements provide private companies with the flexibility to tailor measures to their specific needs and conditions.

These requirements should be aligned with the requirements of the NIS Directive and cover baseline security measures, risk assessment, user awareness, incident response, incident reporting and business continuity management.

### Recommendation 9: Enhance capabilities of public and private actors

After baseline requirements for public and private actors have been defined, existing capabilities need to be evaluated in order to identify gaps and deviations. Where existing capabilities do not conform to national or EU requirements, they need to be developed or enhanced. When evaluating and enhancing capabilities, all four areas from prevention, detection, reaction and deterrence should be considered. Capabilities do include operational measures and technical means but also extend to management systems and necessary resources such as manpower, knowledge, financial resources and a legal foundation.

Governments can actively support capacity building by publishing national standards, designing cyber security capability maturity models, promote and encourage the exchange of knowledge and best practices, providing support and assistance through official agencies, or through state subsidies.

# List of References

Bundesamt für Bevölkerungsschutz BABS (2012): Nationale Strategie zum Schutz kritischer Infrastrukturen. Available online at http://www.babs.admin.ch/de/aufgabenbabs/ski.html

Bundeskanzleramt Österreich (2013): Austrian Cyber Security Strategy. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/austrian-cyber-security-strategy

Center for Cyber Security (2015): The Danish Cyber and Information Security Strategy. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-strategy-for-cyber-and-information-security/at_download/file

ENISA (2008): Raising awareness on information security across public and private organisations.

ENISA (2009): Good Practice Guide on National Exercises. Enhancing the Resilience of Public Communications Networks. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber_exercises/national-exercise-good-practice-guide

ENISA (2010): The new user's guide: How to raise information security awareness. Available online at http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2010/new-users-guide

ENISA (2011): Cooperative Models for Effective Public Private Partnership - Good Practice Guide. Available online at https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps/at_download/fullReport

ENISA (2011): European Month of Network and Information Security for All – A feasibility study. Available online at http://www.enisa.europa.eu/activities/cert/security-month/deliverables/2011/europeansecuritymonth

ENISA (2012): Cyber Europe 2012 – Key Findings Report. Available online at https://www.enisa.europa.eu/publications/cyber-europe-2012-key-findings-report

ENISA (2012): Good Practice Guide on National Contingency Plans for CIIs, available on request.

ENISA (2012): National and International Cyber Security Exercises: Survey, Analysis & Recommendations. Available online at https://www.enisa.europa.eu/publications/exercise-survey2012

ENISA (2013): National-level Risk Assessments. An Analysis Report. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/nlra-analysis-report

ENISA (2014): An evaluation framework for Cyber Security Strategies. Available online at https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

ENISA (2015): ENISA Cyber Europe 2014 – After Action Report. Available online at https://www.enisa.europa.eu/publications/ce2014-after-action-report

ENISA (2015): Latest Report on National and International Cyber Security Exercises. Available online at https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

ENISA (2015): Methodologies for the identification of Critical Information Infrastructure assets and services. Available online at https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

ENISA (2016): Current Risk. Glossary. Available online at http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary

ENISA (2016): Stocktaking, Analysis and Recommendations on the protection of CIIs – Annex. Available online at https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/ciip-governance-in-the-eu-annex

ENISA (2016): Stocktaking, Analysis and Recommendations on the Protection of CIIs. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

European Commission (2012): Update on European Strategy for Cyber Security. Available online at http://www.europarl.europa.eu/document/activities/cont/201207/20120712ATT48826/20120712ATT48826EN.pdf

European Commission (2015): Trust services. Available online at http://ec.europa.eu/information_society/policy/esignature/eu_legislation/regulation/index_en.htm

European Parliament and the Council (1999): Directive 1999/93/EC on a Community framework for electronic signatures. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31999L0093&from=EN

European Parliament and the Council (2013): Directive 2013/40/EU on attacks against information systems. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32013L0040&from=EN

European Parliament and the Council of the European Union (2016): Directive (EU) 2016/1148 of the European Parliament and of the Council. Available online at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

French Senate (2013): Loi de programmation militaire 2014-2019

IT-Security Act (2015): Available online at https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/it-sicherheitsgesetz.pdf?__blob=publicationFile

McKinsey Quarterly (2014): The rising strategic risks of cyberattacks. Available online at http://www.mckinsey.com/business-functions/business-technology/our-insights/the-rising-strategic-risks-of-cyberattacks

National Coordinator for Security and Counterterrorism (2013): National Cyber Security Strategy 2. From awareness to capability. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategy-1/at_download/file

National Cyber Security Centre (2016): National Detection Network. Available online at https://www.ncsc.nl/english/Cooperation/national-detection-network.html

National Security Bureau (2014): National Security Strategy of the Republic of Poland. Available online at http://en.bbn.gov.pl/download/3/1314/NSSRP.pdf

Office of the Commissioner of Electronic Communications & Postal Regulation (2012): Cybersecurity Strategy of the Republic of Cyprus. Available online at https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf

Oxford University Press (2012): Oxford English Dictionary, 7th Edition.

Secretariat of the Security and Defence Committee (2013): Finland's Cyber security Strategy. Available online at https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/FinlandsCyberSecurityStrategy.pdf

Swiss Federal Department of Finance (FDF)[53] (2012): National strategy for the protection of Switzerland against cyber risks. Published under the logo of the Federal Department of Defence, Civil Protection and Sport DDPS. Available online at https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

[53] The Swiss Federal Department of Finance is in charge of the implementation of the NCS and the writing of the NCS II.


## ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

## Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece



Catalogue Number: (TP-05-16-002-EN-N)



PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu



ISBN: 978-92-9204-179-3
DOI: 10.2824/48036