EUROPEAN UNION AGENCY
FOR CYBERSECURITY

BUILDING EFFECTIVE GOVERNANCE FRAMEWORKS FOR THE IMPLEMENTATION OF NATIONAL CYBERSECURITY STRATEGIES

FEBRUARY 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, boost the resilience of the Union's infrastructure, and, ultimately, keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

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

AUTHORS

Anna Sarri, Gema Fernández Bascuñana (ENISA)
Ann-Kristin Gross, Federico Chiarelli, Marina Preasca (Wavestone)

ACKNOWLEDGEMENTS

ENISA would like to thank and acknowledge all the experts that took part and provided valuable input for this report and especially the following, in alphabetical order:

Andrés Jesus Ruiz Vazquez (Spain);
Center for Cyber Security (Denmark), Chief Advisor;
Centre for Cybersecurity (Belgium);
Croatian National Security Authority, Senior Advisor, Vinko Kuculo;
Cyber Security Coordination and Policy Department (the Netherlands), Gijs Peeters;
Cyber Security Coordination and Policy Department (the Netherlands), Pieter van den Berg;
Department for Secure Communication, Senior Advisor and Sweden's Liaison Officer to ENISA (Sweden), Peter Wallström;
Department of Environment, Climate & Communications, Staff Engineer, Cyber Security & Internet Policy Division (Ireland), James Caffrey;
Digital Security Authority of Cyprus, Technical Officer, Costas Efthymiou;
Digital Security Authority of Cyprus, Technical Officer, Giorgos Loninos;
Federal Chancellery, Department I/8 – Cyber Security, GovCERT, NIS-Office and ZAS (Austria), Deputy Head, Christian Zec;
Federal Ministry of the Interior (Germany), Sascha-Alexander Lettgen;
International Server Security Authority (Greece), Head of Competent Department for Cyber Security Strategic Planning, Emmanouil Patsourakis;
International Server Security Authority (Greece), Head of the Directorate for Cyber Security, Ioannis Alexakis;
Malta Information Technology Agency, Katia Bonello;
Malta Information Technology Agency, Martin Camilleri;
Ministry of Home Affairs, Security, Reforms and Equality (Malta);
Ministry of Economic Affairs and Communication, Department of National Cyber Security (Estonia), Kristjan Kaskman;
Ministry of Economic Affairs and Communication, Department of National Cyber Security

(Estonia), Martin Sepp;
Ministry of National Defence of Lithuania;
National Cybersecurity Agency (Italy);
National Cyber and Information Security Agency, National Strategy and Policy Unit (Czech Republic), Tomáš Kellner;
National Cyber Security Centre (Finland), Olli Lehtilä;
National Security Authority (Slovakia).

ENISA would also like to thank them for their valuable contribution to this study, and all the experts that provided input but preferred to stay anonymous.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-604-0

DOI: 10.2824/850466

Catalogue number: TP-04-22-231-EN-N

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

The importance of a sound governance model for the implementation of the National Cybersecurity Strategies (NCSSs) has been highlighted in numerous testimonies of the Member States as well as included in the NIS and NIS2 Directive. However, each country deploys its own governance model with a different level of maturity.

ENISA, taking on its mandate to support and promote the development, deployment and implementation of the NCSS and accompanying governance models, produced this study on "Building Effective Governance Frameworks for The Implementation of National Cybersecurity Strategies". It analyses existing governance models to share a set of good practices when developing a governance model and putting in place the different governance elements.

The proposed governance model consists of four layers with 10 sub-categories, and provides a total of 28 good practices:

- Political governance
  - Political processes;
  - Roles and responsibilities; and
  - Legal measures.
- Strategic governance
  - Strategy itself and its implementation; and
  - Risk identification and mitigation.
- Technical governance
  - International standards and technical guidelines; and
  - Use of technology, tools and certification schemes.
- Operational governance
  - Awareness raising;
  - Incident response; and
  - Information sharing.

The good practices have been defined based on data collected through desk research and interviews with experts and relevant stakeholders from the Member States. The data collected has been analysed to identify trends, and effective instances across the different elements of governance. While the interviews had a European focus with 19 interviews with stakeholders from 18 EU Member States, the geographical scope of the desk research includes a global outreach.

Finally, this report provides insights on KPIs and general indicators to monitor and evaluate the status of implementation of the NCSS and its governance model.

2. ABBREVIATIONS

CERT: Computer Emergency Response Team

CISA: Cybersecurity and Infrastructure Security Agency

CI/CII: Critical Infrastructures/ Critical Information Infrastructures

CSIRT: Computer Security Incident Response Team

ENISA: European Union Agency for Cybersecurity

EU: European Union

GCI: Global Cybersecurity Index

ICT: Information and Communication Technology

IMF: International Monetary Fund

ITU: International Telecommunication Union

KPI: Key Performance Indicator

MITA: Malta Information Technology Agency

MoU: Memorandum of Understanding

NATO: North Atlantic Treaty Organisation

NCAF: National Capabilities Assessment Framework

NCSS: National Cybersecurity Strategy

NGO: Non-Governmental Organisation

NIST: National Institute of Standards and Technology

OECD: Organisation for Economic Co-operation and Development

PPP: Public-Private Partnership

SMEs: Small and Medium-sized Enterprises

UN: United Nations

USA: United States of America

3. INTRODUCTION

With the publication of the Network and Information Security (NIS) Directive[1] in July 2016 and issuing of the draft agreement of the NIS2 in June 2022, the EU Member States have been required to adopt a National Cybersecurity Strategy (NCSS). The NCSS should put forward strategic principles, and guidelines, objectives and priorities to improve and maintain a higher level of security in the context of network and information systems.

In this relation, and as stated by the EU Cybersecurity Act[2], ENISA shall not only support the Member States in developing national strategies but shall also promote the effective deployment of those strategies and support the set-up of a governance model ensuring the sustainability of the NCSS.

As part of its mandate, ENISA publishes a study focusing on the good practices around the set-up and deployment of a governance framework to support the implementation of the NCSS in the EU. The objective of this study is to systematically review existing governance models relevant to the deployment of a NCSS and to identify and select the most relevant instances, lessons learned, and good practices from the EU Member States.

This study aims to collect insights on the definition of processes, roles, and responsibilities, the subsequent deployment of monitoring measures, and to identify the main challenges and good practices that the EU Member States put in place to ensure an effective governance framework for the implementation of NCSSs.

3.1 METHODOLOGICAL APPROACH

The methodological approach used to gather the best practices of governance frameworks relies on four main steps:

1. **Desk Research**: The first step involved conducting an extensive literature review to collect good practices and trends on governance models. The desk research has been focused on good practices adopted in the EU Member States, while insights collected from around the world complement the analysis. A systematic literature review approach has been deployed to review all documents coherently and to methodologically assess the insights of each source in terms of relevance, usefulness, and applicability.
2. **Collection of experts and stakeholders' points of view:** In this context, 19 stakeholders from 18 EU Member States have been interviewed to gain first-hand insights on the status of governance models across the EU Member States, and to identify good practices, as well as challenges, needs and lessons learned. The national stakeholders have all been part of the national authority or government body in charge of the cybersecurity strategy.
3. **Analysis of stocktaking input:** The data collected through desk research and interviews were subsequently analysed to identify good practices in the design of a governance framework.

[1] European Parliament and Council, (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union – NIS Directive, EUR-Lex, available https://eur-lex.europa.eu/eli/dir/2016/1148/oj.
[2] European Parliament and Council, (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – EU Cybersecurity Act, EUR-Lex, available https://eur-lex.europa.eu/eli/reg/2019/881/oj.

4. **Definition of best practices for governance:** Thereafter, good practices and trends in setting up governance models have been defined and validated with national experts, before publication.

The target audience of this study includes policymakers, experts, and government officials responsible for or involved in designing, implementing, and monitoring the NCSS, its processes, actions, and objectives.

4. COMMON ELEMENTS OF GOVERNANCE MODELS

This section defines a common understanding of the concepts of governance, cyber governance, and governance models. Moreover, it highlights the main results and insights from the literature review conducted on the topic of governance models of NCSS. By doing so it outlines the main elements of different levels of governance and builds the framework for analysis leveraged on in chapter 5.

4.1 DEFINITION OF GOVERNANCE, CYBER GOVERNANCE AND GOVERNANCE MODELS

The desk research on governance models included 49 sources, reaching from academic and scientific articles, over reports, to guides on how to develop governance models as well as governance models themselves. The main focus of the geographical scope has been the EU, nevertheless, inputs from other countries (e.g., USA) have been considered to ensure a wide array of results and to also take into account the developments in other parts of the world.

4.1.1 Governance

The term governance is used in a plethora of different topics and different contexts. Following the vast amount of available literature on the topic of governance, there is not one, all-encompassing definition that would hold across its different areas of application. Rather, multiple but complementary, partly overlapping definitions exist to describe and detail what 'governance' entails.

Stemming from the original meaning of 'governing' in the context of individual rule it is and has been used throughout time often about institutional structures. The concept originally describes actions and processes to lead, structure, and enable institutions and organisations to exist, function, and persist. Only recently, governance has been related to international institutions and gained popularity. It has started to be used by international organisations such as the European Union, World Bank, the International Monetary Fund (IMF), and the Organisation for Economic Co-operation and Development (OECD) more frequently. Further, it has been stated that since the concept has gained more popularity, governance became one of the most controversially discussed topics when it comes to democracy theory and democratisation.[3] Governance is predominantly seen as:

- a process to coordinate a network of stakeholders with independent positions, opposing and conflicting opinions and interests;
- a mechanism to steer and control society, and results from the interaction of political, economic and social actors;
- a complex system including different stakeholders from the public administration, the private sector and non-governmental organizations, influenced by interactions thereof; and

[3] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

- a triangle composed of participation, transparency and accountability and creates a framework "regulating socio-economic conditions, developing social and physical infrastructures, and providing social security nets".[4]

For the remainder of this study, we will use the following definition of governance:

> *Governance describes a complex system, defining roles, responsibilities, processes and relationships between involved actors. Governance includes stakeholders from the private sector, public administration as well as civil society and spans over different topics such as economic, social and political priorities.*

4.1.2 Cyber governance

The domains of cyber, cybersecurity and cyber threats experienced increasing importance, and cyber governance became a popular topic. While the field of cyber or 'cyberspace' describes the environment consisting of the global information systems and their connecting network, cybersecurity entails the prevention of damage and the protection against attacks on, among others, computers, information and communication systems as well as processes, data, hard- and software.[5] Threats in the cyberspace arise from attacks on the processed information or the systems themselves. Cybersecurity is also part of the cyberspace and aims at securing the confidentiality, integrity, accessibility, availability and privacy of the information processed, stored and used.[6] Given the interconnections in the cyberspace, cybersecurity cannot be assessed, analysed or described without taking into account other aspects of cyberspace as well.

The functioning of the cyberspace depends on various stakeholders, processes and elements within cyber governance. International organisations started to find solutions for challenges related to cyber governance, for example developing and signing the 'Cyber Crime Convention''.[7] In addition, international standardisation has been adopted, i.e., ISO/IEC 38500:2015 providing guiding principles[8] for governing bodies' members on "effective, efficient and acceptable use of IT in their organizations".[9]

Definitions of cyber governance are emerging and describe it as the

> *"Operation of decision-making processes" which increase and ensure "participation, transparency, and accountability in taking measures related to cyberspace together with the mechanism of international agreements, strategies, laws, measures, regulations, and standards that interlock in the best way".*[10]

This definition will be used for the remainder of this study.

4.1.3 Governance Models

Similar to the definition of governance, a single definition of the governance model is not agreed upon in the literature. Different types, descriptions and definitions have been developed covering different levels of granularity. This section aims to provide an overview of the current state of the art of developing governance models. To this end, structured desk research has

[4] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[5] NIST Computer Security Resource Center, Glossary, last updated 2022, available https://csrc.nist.gov/glossary.
[6] NIST Computer Security Resource Center, Glossary, last updated 2022, available https://csrc.nist.gov/glossary.
[7] Council of Europe, Impact of the European Convention on Human Rights – Budapest Convention, Council of Europe Portal, 2001, available https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/.
[8] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[9] ISO, ISO/IEC 38599:2015 Information technology – Governance of IT for the organization, 2015, available https://www.iso.org/standard/62816.html.
[10] Efe, A. & Bensghir, K. T., cited in Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

been conducted focusing on the development and set-up of governance models in general, and specifically, the ones related to the implementation of NCSSs.

In the literature, two main patterns of defining governance models are predominant, one focusing on the different layers of governance and one targeting the stakeholders and objectives of the model. An advantage of the latter is that overarching and transversal activities can be integrated, analysed and evaluated. However, this might come at the expense of the accuracy of the definition of the roles and responsibilities of the stakeholders involved and their accountability. The Government Cyber Security Strategy of the British Government employs this path in defining its governance model and focuses on the overall objectives of the implementation of the cybersecurity strategy.[11]

Defining a governance model based on its different layers might increase the overall complexity of the framework, however, this option yields several benefits, including a more thorough description of its components (e.g., stakeholders, objectives, etc.). In addition, it is possible to provide a clear allocation of responsibilities and describe more detailed channels of communication, information exchange and collaboration. The different levels of governance include the political aspect, definition of processes, roles and responsibilities, operationalisation of actions and their technical implementation. The Global Cybersecurity Index divides governance models into legal, technical, organisational, capacity development and cooperative measures.[12] Similarly, cybersecurity governance in some US States focuses on the following areas of governance, as identified by the Department of Homeland Security: Strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, workforce and education.[13]

This report will follow the majority of sources analysed and will define governance models along different levels or layers. This allows the provision of a more granular assessment of governance models. The elements of the framework such as objectives, stakeholders and actions can be described per level, providing a holistic approach to their definition.

While governance can be divided into a variety of levels, most sources assessed governance along similar layers. Based on the conducted desk research four main levels of governance have been identified as predominant, thus, these were selected to build the governance framework of this report:

a) Political governance;
b) Strategic governance;
c) Operational governance; and
d) Technical governance.

The next section will provide an overview of the main elements driving each of the four levels of governance.

4.2 THE STATE OF ART OF GOVERNANCE MODEL FOR NCSS

In general, political governance is the most thoroughly covered level of governance in literature. Specifically, the set-up of processes and the allocation of responsibilities to ensure a successful governance framework are the most prominent elements.[14] In addition, elements concerning

[11] UK Cabinet Office, Government Cyber Security Strategy: 2022 to 2030, policy paper published by the UK Government, 2022, available https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.
[12] ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021.
[13] Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications.
[14] Among others: ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021; Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4; Sutherland,
[1] Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

incident response in the context of operational governance have been pointed out by several sources.[15] While their importance is highlighted and aspects are clearly defined, elements of the strategic and technical layers are less thoroughly covered.

In addition to the main elements governing the different levels of governance, the literature emphasises the importance of monitoring mechanisms across all levels. Their establishment along with the ones of key performance indicators (KPIs) or other measures for coherent evaluation is important for the successful implementation of NCSSs. Chapter 6 covers the monitoring of governance models in detail.

The remainder of this chapter will highlight the findings and point out the identified trends from the desk research across the four levels of governance: political, strategic, operational and technical. This provides the framework for the analysis carried out under chapter 5, which focuses on the inputs shared by the Member States.

4.2.1 Political governance

Political governance provides a framework of defined processes and relationships as well as legal guidelines. It establishes the formal angle of governance and is often seen as governance itself, as it is tightly related to the execution of political actions and entails governing, leading and overseeing processes and actions implemented. The main objective of the political layer is the establishment of processes, roles and responsibilities to ensure the implementation of the NCSSs and their related policies. In turn, official processes, clearly defined roles and proper legal measures foster the creation of accountability, ensure transparency and facilitate the acceptance of the NCSSs among all the relevant stakeholders.

Political bodies, such as dedicated cybersecurity agencies or departments within different ministries are leading the political level. Hence, oftentimes, decision-makers are included in some of the processes to ensure accountability and political acceptance. Other actors actively participating in building and executing political governance are academia, consultancies and other expert bodies, which provide topical expertise and support to political actors in setting up, organising and executing political governance. Public-Private Partnerships (PPPs) play an important role in the enforcement and accountability of political governance, as they help build bridges between the private and the public sector, ensuring the implementation of actions responding to industry needs.[16]

Common elements of political governance can be clustered into three main groups, as defined in Figure 1, namely: i) Political processes, ii) Roles and responsibilities, and iii) Legal measures.

E. Cybersecurity: Governance of a New Technology, in: Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018, SSRN, 2018, available https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148970; NIST, Cybersecurity Framework, NIST Publications, 2018, available, https://www.nist.gov/cyberframework/resources; NIST, Success Stories – Israel National Cyber Directorate v. 1.0, 2020, available https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-20, NIST Success Stories – Japanese Cross-Sector Forum, 2020, available https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum.

[15] Among others: Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications; ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021; Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/; ENISA, NCSS Good Practice Guide, ENISA Publications, 2016, available https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

[16] ENISA, Public Private Partnerships (PPP) – Cooperative models, ENISA publications, 2018, available https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models.

Figure 1: Main elements of political governance

Source: Authors' own elaboration.

In general, political governance seems to be the most advanced of all four levels of governance, in fact, measures to define political processes, roles and responsibilities seem to be most actively discussed and analysed by the literature. Legal measures are not equally assessed, however, their importance is vital as they set the basis for the country's legal framework and the obligations of the different stakeholders.

Political Processes

Among the elements of political processes, particular emphasis is put on initiating cooperative and collaborative approaches and ensuring joint dialogues. In this context, the inclusion and active participation of various stakeholder groups across different levels has been stressed[17], together with the creation and active integration of PPPs in the political processes given their contribution in actively shaping the implementation, monitoring and evaluation of NCSSs.[18] Additionally, the importance of inter-sectoral cooperation has been highlighted due to the possibility of creating synergies and ensuring commitment to the implementation of actions among stakeholders.[19]

In addition, cooperation and collaboration across the different governmental institutions are essential to guarantee a coherent approach towards the implementation of the NCSSs. Intra-governmental coordination and cooperation are considered core functions and prerequisites for functioning governance mechanisms, such as the application of standards, regulations and market incentives. Hence, cooperation between government institutions is ultimately important

[17] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4; NIST Success Stories – Japanese Cross-Sector Forum, 2020, available https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum.
[18] ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021.
[19] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.

to ensure that the desired outcomes are met, and that the objectives of the governance model and the strategy are fulfilled.[20]

Lastly, international cooperation and collaboration have been pointed out as highly important. It has been stated that, given the international character of the cyberspace, a complete solution for cyber governance cannot be based on national understanding alone, but needs to be embedded and coordinated in the international arena.[21] Further, international cooperation, collaboration and exchange on the set-up of a governance model will benefit all parties through the development and improvement of cyber governance. In this regard, the development of an international common language for cyber defence is considered an immediate necessity to enable international exchange among experts.[22]

Definition of roles and responsibilities

After the political processes, the definition of roles and responsibilities is the most covered aspect in literature. All stakeholders must have clearly allocated roles, and responsibilities to ensure the successful implementation of the strategy and achieving its objectives.[23] In this relation, it has been mentioned that personnel and financial resources should be clearly defined and allocated. The clear allocation of responsibilities is important to ensure accountability of the responsible actors, while the clear allocation of roles is important to set up an effective and efficient governance system and avoid overlapping of mandates.

A common trend emerging from desk research is the setting-up of a lead authority or body. While different options can be deployed to do so, a central body or actor taking the main coordinating responsibilities and roles seems beneficial and is important to allocate actions and monitor the progress of implementation.[24] There are three commonly applied options: building an entirely new body dedicated to the implementation of the NCSS; expanding the mandate and the responsibilities of an already existing central body; or extending the responsibilities of several decentralized political entities, such as ministries. In addition, working groups on different topics might be established to enable engagement across bodies and entities involved.[25] They facilitate and develop formalized cooperation mechanisms to enable international collaboration.[26] Finally, the establishment of an advisory council built by academic and industry experts to be consulted by responsible government officials has been pointed out as particularly beneficial.[27]

Another option refers to the partial or full outsourcing of the cybersecurity services to PPPs by establishing them as stand-alone organisations. This is particularly helpful if the government misses the expertise or capacity to react to the identified needs for action. The PPPs provide

[20] Sutherland, E. Cybersecurity: Governance of a New Technology, in: Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018, SSRN, 2018, available https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148970; Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/
[21] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[22] NIST Computer Security Resource Center, Glossary, last updated 2022, available https://csrc.nist.gov/glossary.
[23] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/; Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[24] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/; Sutherland, E. Cybersecurity: Governance of a New Technology, in: Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018, SSRN, 2018, available https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148970; NIST Computer Security Resource Center, Glossary, last updated 2022, available https://csrc.nist.gov/glossary.
[25] ENISA, National Cyber Security Strategies: An Implementation Guide, ENISA Publications, 2012, available https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.
[26] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[27] Marsh & McLennan, MMC Cyber Handbook 2021 – Cyber Resilience Perspectives: Clarity in the midst of Crisis, MarshMcLennan Publications, 2021, available https://www.marshmclennan.com/insights/publications/2020/october/mmc-cyber-handbook-2021-.html.

cybersecurity services, while the national public authorities remain in an overseeing position.[28] The different set-ups of and the collaboration with PPPs are widely discussed, and there is a common agreement on the strategic importance of including them within the NCSS and its governance model. The organisation, structure and legal basis of PPPs differentiate from country to country, however, a common factor pointed out by several sources is the relevance of including governmental and private sector representatives (e.g., SMEs) in the PPP decision-making process.[29]

Legal measures

Regarding legal measures for governance models, it has been stressed that the establishment of a legal framework or a legal governance system is important to provide guidance and support. Additionally, the existence of legal measures provides legally binding mandates and ensures enforcement, accountability and transparency during the implementation process.[30] On implementing legal measures, it has been specified that they should be built in a far-sighted approach to be able to accompany future changes brought by digitalisation.[31]

To support the cooperative and collaborative approach, legal measures should be inclusive and have general validity, to ensure that all institutions, organisations and related stakeholders are committed to the NCSS, its governance model and the implementing actions. Legal measures also help giving policies and actions for the implementation of a governance model a binding character and are hence essential tools of a complete governance model.[32]

In line with the importance of setting up international cooperation and collaboration, the legal framework should reflect this by international guidelines and cooperation on the definition of legal measures internationally. Lastly, it is emphasised that human rights should be tightly connected to and taken into account in all processes of setting-up a cybersecurity governance model, but specifically related to the legal framework. Of particular importance is ensuring trust, transparency, and equity through the legal framework.[33]

4.2.2 Strategic governance

Strategic governance describes the level of governance directly linked to the NCSS. It is important to tightly connect the processes of designing the strategy and designing its governance model to ensure continuity and coherence. Strategic governance targets linking and coordinating the processes of drafting the strategy and building the governance model from the outset. Additionally, strategic elements of identifying and mitigating risks necessitate strong cooperation and collaboration between actors involved in both, the governance model, as well as the strategy development.

The main stakeholders involved in the strategic governance level are political actors drafting the strategy. Often, working level government officials are main actors here, while higher level government officials are involved for validation, acceptance, accountability and enforcement purposes. Political actors are often supported by working groups, consulting bodies and other

[28] Marsh & McLennan, MMC Cyber Handbook 2021 – Cyber Resilience Perspectives: Clarity in the midst of Crisis, MarshMcLennan Publications, 2021, available https://www.marshmclennan.com/insights/publications/2020/october/mmc-cyber-handbook-2021-.html.
[29] ENISA, Public-Private Partnerships (PPP) – Cooperative models, ENISA publications, 2018, available https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models..
[30] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.
[31] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[32] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.
[33] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4; Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.

stakeholders providing expertise to draft the strategy and corresponding implementation actions.

Overall, three clusters have been identified in which the main elements of strategic governance can be grouped, namely elements concerning: i) the strategy itself, ii) the implementation of the governance model, iii) strategic aspects of risk identification and mitigation. Figure 2 illustrates them.

Figure 2: Main elements of strategic governance

Source: Authors' own elaboration.

Elements concerning the strategy itself and the implementation of a governance model

Firstly, the literature on strategic governance emphasises that already at the set-up stage of the strategy, the development of a governance framework should be taken into account and included in the strategy. Drafting the strategy and at the same time already including possible operational, political and legal measures, which should be put in place for the strategy's implementation, is argued to be beneficial, as processes and timelines are streamlined.[34]

Secondly, after the strategy has been drafted, the implementation should be guided by an implementation plan to point out specific actions and ensure the support of the strategy across the different governmental and civil society levels.[35]

Thirdly, thorough planning and a clear indication of the overall planned priorities, the foreseen budget and resources is important to integrate the implementation of cybersecurity in the general national planning and governance approaches. It is important to align priorities of the

[34] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.
[35] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/; ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021; Marsh & McLennan, MMC Cyber Handbook 2021 – Cyber Resilience Perspectives: Clarity in the midst of Crisis, Marsh McLennan Publications, 2021, available https://www.marshmclennan.com/insights/publications/2020/october/mmc-cyber-handbook-2021-.html.

cybersecurity strategy with other governmental priorities on national level. This fosters commitment and support from different bodies, and actors across the government.[36]

Risk identification and mitigation

Regarding the strategic elements of risk identification and mitigation, it has been stressed that a coherent approach across all government entities and critical infrastructure operators should be aimed for. Having a sound approach for risk identification and mitigation, which is coherent across the different actors, facilitates exchange and information-sharing and fosters cooperation.[37] In fact, the creation of specific agencies providing services of risk identification and mitigation has been pointed out, as centralizing these aspects facilitates exchanges. However, challenges related to accountability, transparency and the protection of human rights. This should be taken into account and mitigated from an early stage of the strategy.[38]

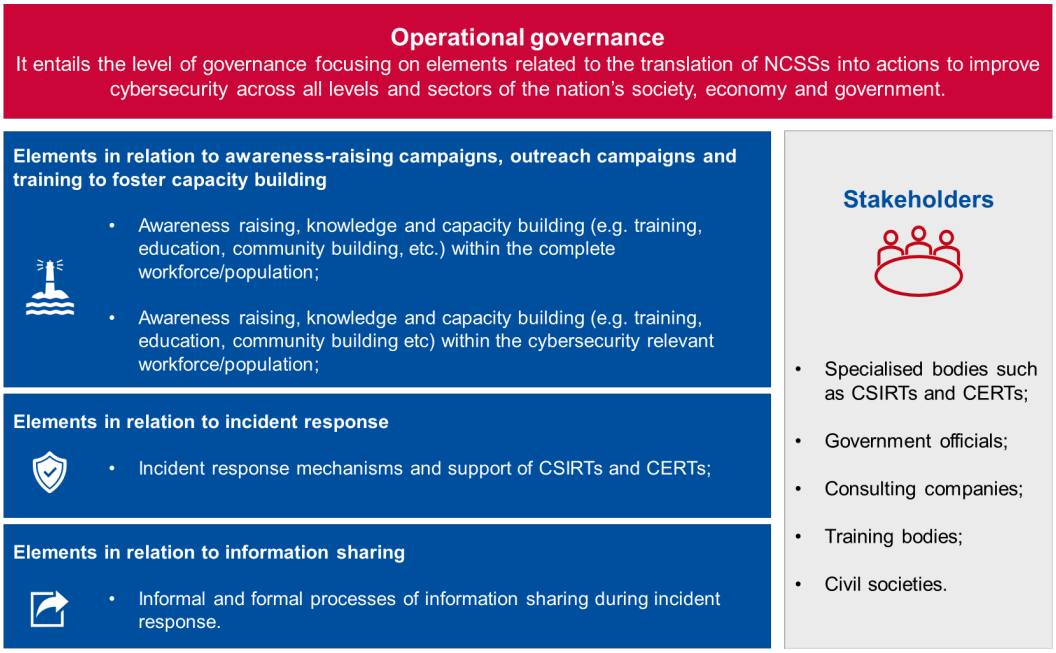
4.2.3 Operational governance

Operational governance entails the level of governance focusing on elements related with the translation of NCSSs into actions to improve cybersecurity within the country. The objective of the operational governance level is to increase cybersecurity across all sectors of a nation's society, economy, and government. The main group of stakeholders, actively involved in the set-up and execution of this governance layer includes specialised bodies such as Computer Security Incident Response Teams (CSIRTs) and Computer Emergency Response Teams (CERTs), government officials and consulting and training bodies. Nevertheless, it is important to mention that the complete society and population is connected to this level of governance. Effectively improving cybersecurity can only be successful if the general public of a country is included and capacity and community-building efforts are undertaken across society.

As pointed out, some aspects falling under the operational governance level are well covered in literature on governance models. This applies particularly to aspects in the context of incident response and capacity-building.[39] During the desk research, three main clusters governing operational governance have been identified: i) awareness-raising campaigns, outreach campaigns and trainings to foster capacity-building, ii) incident response, iii) information sharing and channels Figure 3 illustrates them:

[36] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/; Marsh & McLennan, MMC Cyber Handbook 2021 – Cyber Resilience Perspectives: Clarity in the midst of Crisis, Marsh McLennan Publications, 2021, available https://www.marshmclennan.com/insights/publications/2020/october/mmc-cyber-handbook-2021-.html.
[37] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.
[38] Sutherland, E. Cybersecurity: Governance of a New Technology, in: Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018, SSRN, 2018, available https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148970; Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications.
[39] ENISA, NCSS Good Practice Guide, ENISA Publications, 2016, available https://www.enisa.europa.eu/publications/ncss-good-practice-guide; Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4; Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/; ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021; Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications.

Figure 3: Main elements of operational governance



Source: Authors' own elaboration.

Awareness raising campaigns, outreach campaigns and trainings to foster capacity-building

Awareness raising and outreach campaigns accompanying the implementation of NCSSs foster the acceptance and uptake of cybersecurity measures. It is of utmost importance to train stakeholders, which are involved either directly with the set-up or implementation of the strategy or involved in combating cybercrime.[40] Nevertheless, there is a strong trend incentivising the creation of initiatives to raise awareness within the general population. Through explaining "why", "how" to use certain standards, tools and technologies, or "what" to do and "why" to do so, would increase the safety of the general population.

In this sense, it has been repeatedly stated that not only stakeholders and actors directly working with the NCSSs should be targeted by education campaigns and trainings, but that instead the whole population, starting from a young age, should be integrated in these activities to close the 'cyber skill gap'.[41] This would be important to ensure success of the NCSS, as huge cyber risks emerge from untrained persons, which are not aware of risks or how to protect against cyber threats effectively. A more holistic approach should be taken in order to build a cybersecurity culture and enhance capacity- and community-building across the population. In this way, by shifting away from pure information-sharing and problem-related approaches, cybersecurity could yield efficiency and performance gains for the private sector and the national economy.[42]

Incident response mechanisms

Operational governance is also driven by formalised mechanisms for incident response. Literature suggests the creation of CSIRTs and CERTs to provide support in case of cybersecurity incidents. Specialised teams dedicated to cybersecurity mechanisms should be

[40] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.
[41] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4; Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications; NIST Computer Security Resource Center, Glossary, last updated 2022, available https://csrc.nist.gov/glossary.
[42] ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021.

implemented, driven by thorough action plans in case of incidents.[43] CSIRTs and CERTs provide a centralised contact point on national level and enable a quick and systematic reaction during incidents. CSIRT and CERT bodies should hence take proactive as well as reactive functions and measures to not only support during incidents, but to also prevent incidents from happening and support countries in learning from experience to build resilience against cyberthreats.[44]

Information sharing

Setting-up formal information-sharing programmes as well as defining possible informal information-sharing programmes through an operational framework would foster effective and consistent coordination.[45] Trusted relationships are highly important, more specifically, the development of informal networks would be highly beneficial as information-sharing based on personal interests is most authentic.[46] However, trusted relationships need time to develop and hence, the involvement of different stakeholders and close cooperation from the start seem to be important.[47] Additionally, according to research, shaping information-sharing processes should be supported by CERTs and CSIRTs.[48]

For a successful incident response, it is highly important in this context to firstly define clearly what a cybersecurity incident constitutes, and how processes, roles and responsibilities are allocated and performed during an incident.

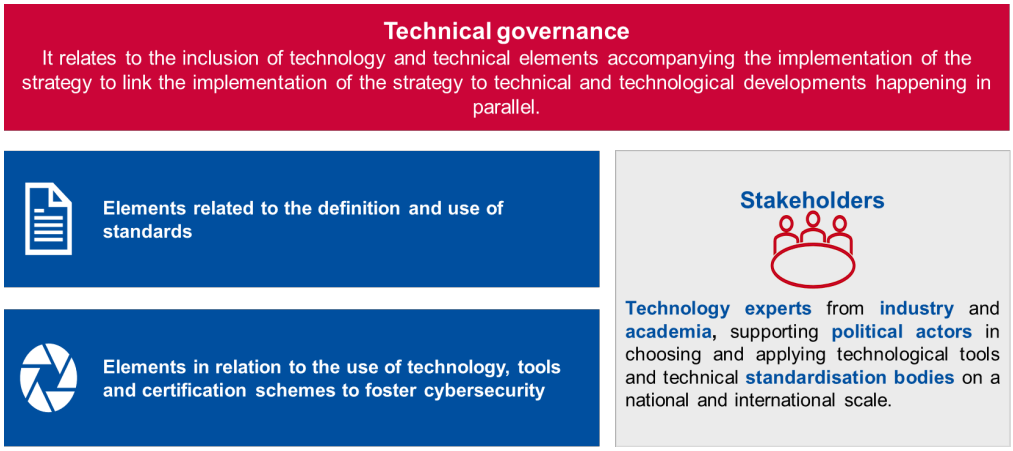
4.2.4 Technical governance

The technical level of governance relates to the inclusion of technology and technical elements accompanying the implementation of the strategy. Its objective is to link the implementation of the strategy to technical and technological developments happening in parallel. This is particularly important in the cyberspace, a fast-evolving field, in which new threats and challenges arise at the same time of new technological possibilities and solutions. The main stakeholders involved in this level are technology experts from industry and academia, supporting political actors in choosing and applying technological tools as well as technical standardisation bodies on a national and international scale.

Currently, the elements of technical governance are covered least in the literature and seem to not yet been heavily focussed on. Although some trends have been identified, due to the low coverage of technical aspects across literature, these trends might not be representative, given the fast technical advancements and developments. Two main clusters of elements governing technical governance have been identified during the desk research: i) definition of standards and specification, and ii) use of technology, tools and certification schemes to foster cybersecurity. They are illustrated in Figure 4.

[43] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/.
[44] ITU, Global Cybersecurity Index, ITU Publications, 2021, available at https://www.itu.int/pub/D-STR-GCI.01-2021.
[45] Cybersecurity foundation, The NCS Guide 2021, 2021, available https://ncsguide.org/the-guide/
[46] Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications.
[47] Cybersecurity & Infrastructure Security Agency, Cybersecurity Governance Publications, CISA Publications, 2017, available https://www.cisa.gov/publication/cybersecurity-governance-publications.
[48] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

Figure 4: Main elements of technical governance



Source: Authors' own elaboration.

Standardisation

The use and definition of standards has been emphasised in order to build a technical governance framework for cybersecurity. Particularly important in this relation would be the use of international and global standards to not only provide technical guidelines but to base cybersecurity governance on existing and globally established technical standards.[49]

Use of technology, tools and certification schemes

The technical layer also includes the undertaking of appropriate and proportionate technical and organisational measures to manage risks. To this end the NIS2 directive emphasises the importance of certification schemes and stresses the importance for the Member States to require essential and important entities to certify certain ICT products, ICT services and ICT processes under specific European cybersecurity certification schemes.

Moreover, CSA article 58 defines mandatory obligations for the Member States to designate NCCAs (National Cybersecurity Certification Authorities) or to reuse the existing NCCA of another Member State, as to supervise certification; this entails the implementation and assessment of the technical governance activities related to such obligations (which entity has been designated, to which ministry it belongs, how it is staffed, how it interacts with other national authorities having a cybersecurity role, etc.).

A second main element emerges from the use of technology and tools to support the set-up of a governance model and the implementation of the NCSSs. Updating tools and technologies used in industry, by the government or other communication systems, can support reaching the NCSS's objectives. In addition, technology and tools such as mobile devices can not only support security but can also provide technological guidance and open possibilities to promote human rights in the sphere of cybersecurity.[50] However, if not updated, tools and technology may pose risks to cybersecurity.

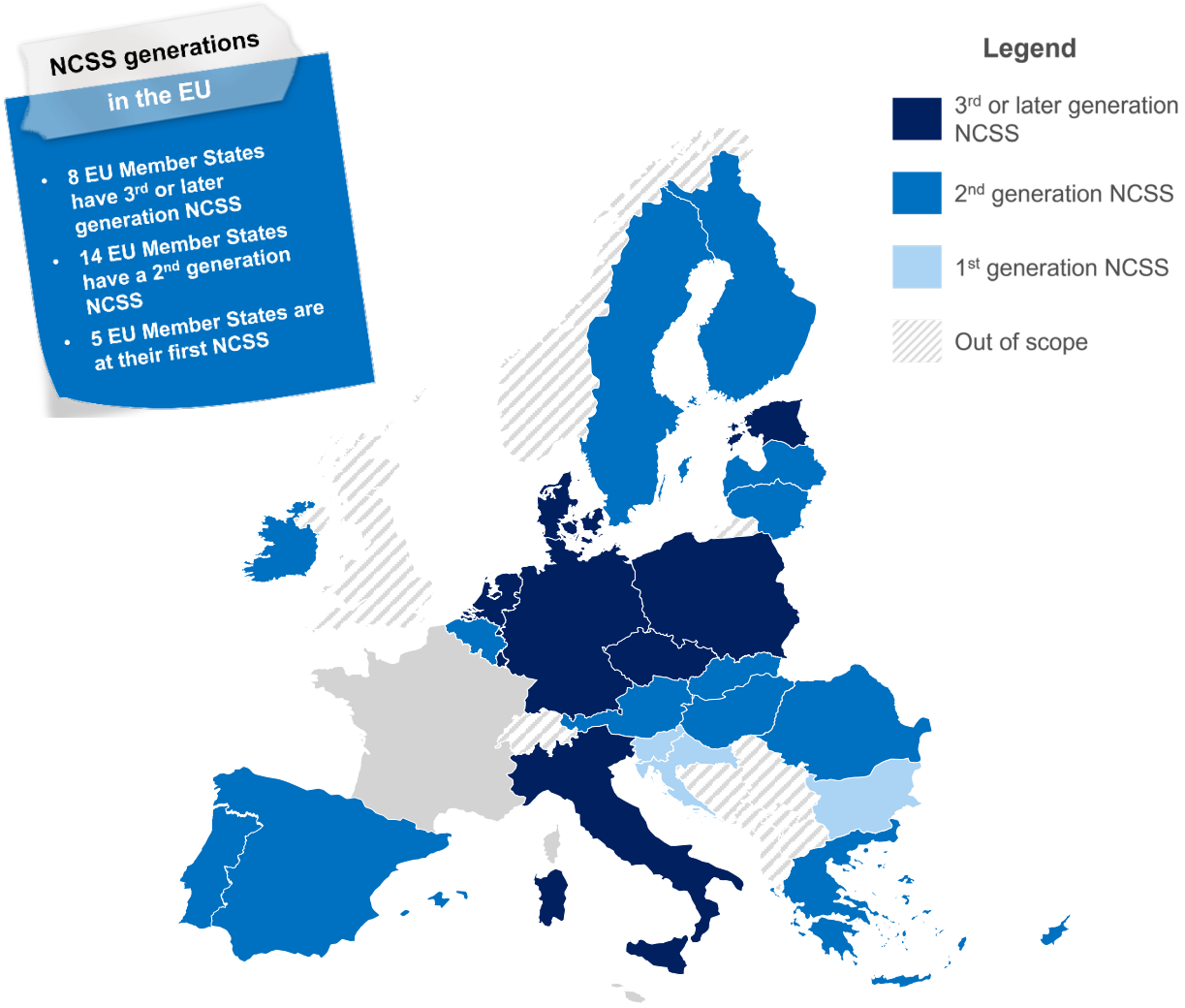
[49] NIST, Cybersecurity Framework, NIST Publications, 2018, available, https://www.nist.gov/cyberframework/resources; NIST, Success Stories – Israel National Cyber Directorate v. 1.0, 2020, available https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-20; Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

[50] Savas S. & Karatas, S. Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

4.3 THE STATE OF THE ART: STATUS OF THE NCSS ACROSS THE EU MEMBER STATES

Currently, all EU Member States have a NCSS in place. Figure 5 below showcases the status of each country of developing updated versions and new editions of their NCSS.

Figure 5: State of Art: NCSSs across the EU Member States

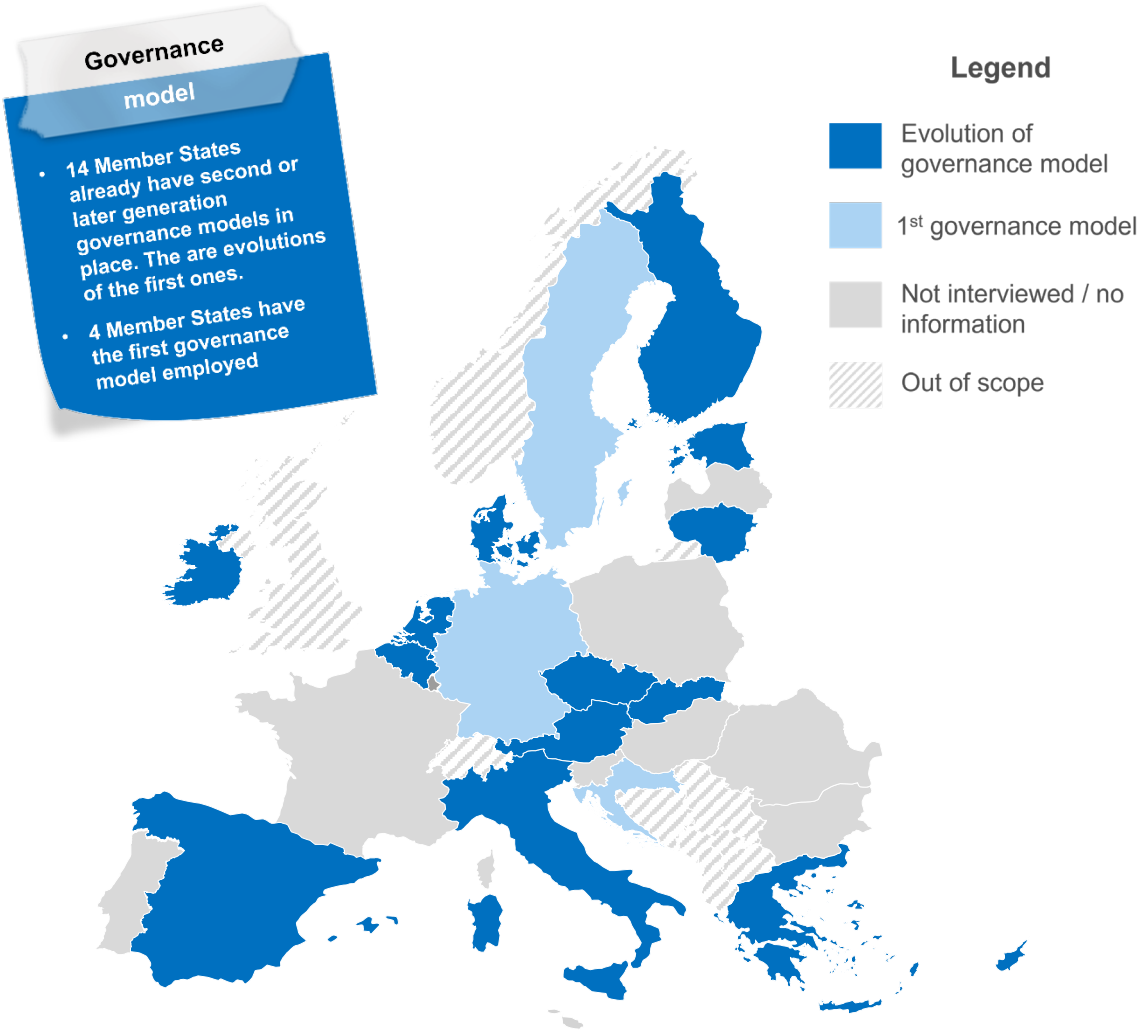


Source: Authors' own elaboration.

All 18 Member States[51] interviewed for this report have currently a governance model in place to support the implementation of the NCSS. Similarly, all Member State representatives stated that having in place a governance model is highly important when implementing the NCSS. Figure 5 provides an overview of the EU Member States which have deployed their first NCSS governance model and highlights in a darker blue those countries which already employed later editions of the governance model. In general, it can be said that the NCSSs are updated every three to seven years. The governance model would need to be updated as well, taking into account recent developments in the cyberspace due to its close relationship with the NCSS.

[51] The following Member States have been interviewed during this study: Austria, Belgium, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Germany, Greece, Ireland, Italy, Lithuania, Malta, the Netherlands, Slovakia, Spain, Sweden.

Figure 6: State of Art: Deployment of governance models for NCSS across the EU Member States



Source: Authors' own elaboration.

From Figure 6, it can be noticed that some countries introduced an accompanying governance model over the years, and that some countries introduced it only after the first NCSS was already deployed. While this shows that the Member States used to have different approaches to implementing their NCSSs, it also indicates growing agreement of the importance of setting-up a governance model. It is interesting to notice that maturity of the governance model does not necessarily depend on or correlate with the number of further editions of the NCSS.

5. SETTING UP A GOVERNANCE MODEL

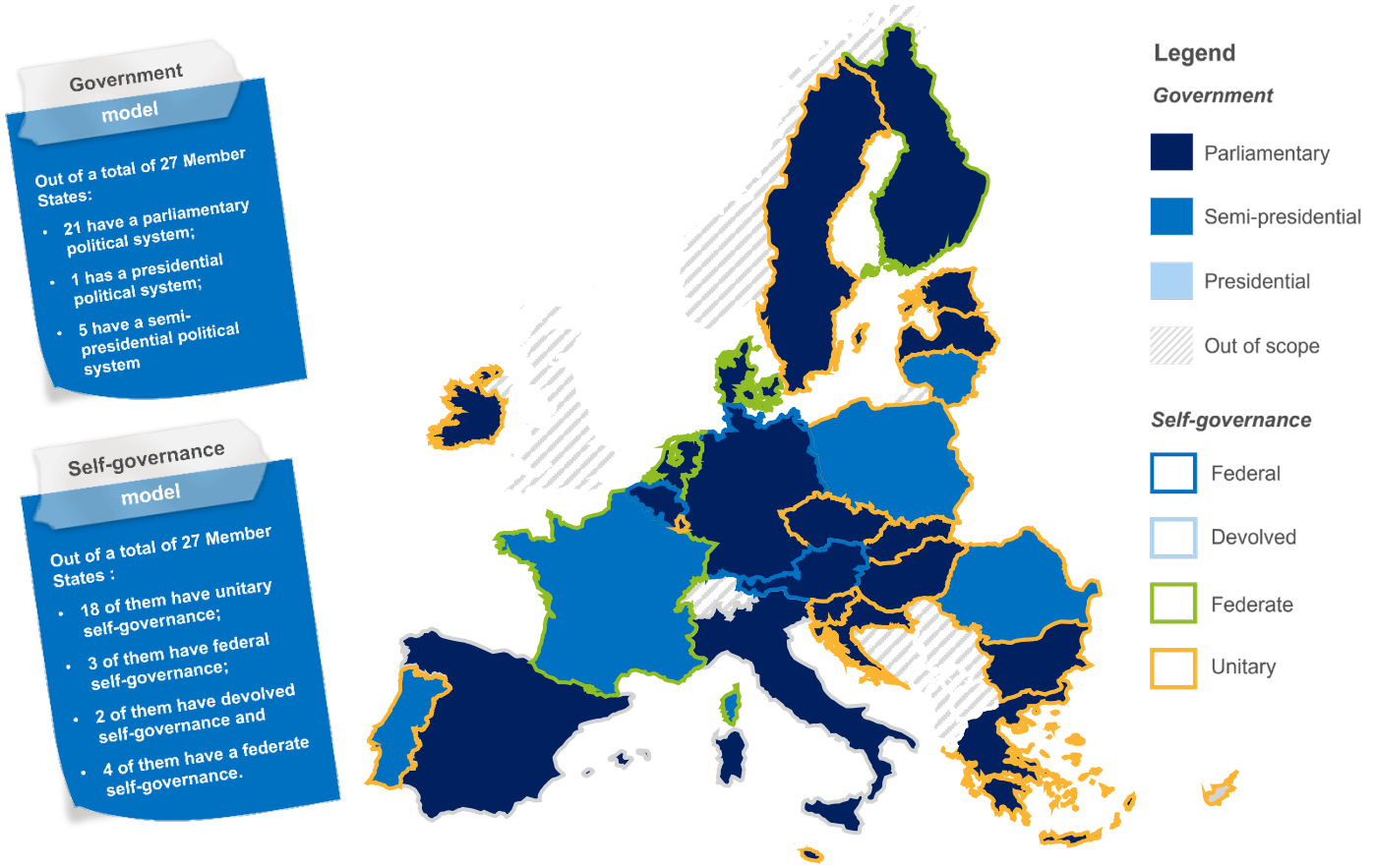
Following the identification of the different levels of a governance model, this section will focus on the analysis of the different elements of each layer and will highlight the good practices shared by the Member States' representatives during the conducted interviews.

Before diving into the different governance models, it is important to have an overview of the political systems of the EU Member States to understand whether this factor influences the selection of a specific governance model. Figure 7 illustrates the model of government and self-governance of the Member States. Regarding the government model, out of a total of 27 Member States, 21 countries have a parliamentary political system[52], one has a presidential political system[53] and five have a semi-presidential political system[54]. While, with regard to the self-governance model, out of a total of 27 Member States, 18 of them have unitary self-governance[55], three of them have federal one[56], two a devolved self-governance[57] and four of them have a federate one[58].

To analyse the relation between a country's government model, self-governance structure and the type of governance model of the NCSS currently deployed, the different governance models highlighted during the interviews have been mapped against desk research on government and self-governance types. It has been noted that there is no correlation between the type of government, self-governance, and the governance model of the NCSS. In fact, there are several additional factors that influence its definition. For instance, the size of a country, its level of maturity in the cyber domain, and the level of cooperation with the private sector, just to name a few. This finding led to the conclusion that it is not possible to have a unique governance model to be used as a reference. Therefore, in this chapter, for each element of the different levels of governance, good practices rather than a governance model will be shared.

[52] A parliamentary political system is a democratic form of government in which the party (or a coalition of parties) with the greatest representation in the parliament (legislature) forms the government, its leader becoming prime minister or chancellor.
[53] A presidential political system is a form of government in which a head of government, typically with the title of president, leads an executive branch that is separate from the legislative branch in systems that use separation of powers.
[54] A semi-presidential political system is a system of government in which a president exists alongside a prime minister and a cabinet, with the latter two responding to the legislature of the state.
[55] A unitary state is a system of political organization in which most or all the governing power resides in a centralized government.
[56] A federal self-governance is characterized by a union of partially self-governing provinces, states, or other regions under a central federal government (federalism).
[57] A devolved self-governance is a statutory delegation of powers from the central government of a sovereign state to govern at a subnational level, such as a regional or local level. It is a form of administrative decentralization.
[58] A federated state is a territorial and constitutional community forming part of a federation. Such states differ from fully sovereign states, in that they do not have full sovereign powers, as the sovereign powers have been divided between the federated states and the central or federal government.

Figure 7: Member States' political system of governance



Source: Authors' own elaboration.

In the preliminary phase of the interviews, the Member States shared the key elements influencing the national approach to the governance model of their NCSS, as well as the main challenges faced during its deployment. The key challenges have been assessed and grouped to provide an overview of the main challenges, experienced by several of the Member States. Table 1 presents the key challenges while Table 2 provides an overview of the related lessons learnt. It can be noticed that the most underlined difficulties are related to the definition of roles and responsibilities, the lack of coordination and cooperation as well as the challenge in reaching a common agreement between the different stakeholders.

Table 1: Key challenges when deploying the governance model

	Key Challenges
1	**Definition of roles and responsibilities** Given the number of stakeholders involved, a lack of understanding of the different roles in the overall picture and duplication of efforts may happen.
2	**Lack of coordination and cooperation** Given the complex structure of some National Cybersecurity systems, the existence of several security authorities including regional competent authorities, coordination, and cooperation between the different actors is a challenge.
3	**Reach a common agreement on the strategy** Given the number of stakeholders involved, reaching an agreement on both, the main goals of the strategy and its phrasing, seems to be difficult.

	Key Challenges
4	**Information sharing** Given the number of different stakeholders involved in the implementation of the strategy, and therefore, included in the governance model, there were some difficulties in sharing information among the different actors. Considering the constantly changing field of cybersecurity, the flow of information is sometimes too slow, especially in terms of regulation and organisation.
5	**Definition of the overall strategy's budget** Considering the decentralized governmental approach of some countries, significant delays may occur in receiving the budget or in obtaining a dedicated budget.
6	**Achieve a higher level of national cyber security and resilience** Given the increasing cyber risks and the global geopolitical situation, some Member States are struggling to cope with the new cyber challenges.
7	**Timeline of the development and implementation of the NCSS** In fact, it would be more beneficial to develop and approve the implementation plan and to define the governance model, at the same time as the NCSS.
8	**Lack of enthusiasm** Given that for some stakeholders the cybersecurity strategy is an extra workload while they are already engaged in numerous other activities, a lack of enthusiasm and motivation could be noticed, which indirectly hinders the good performance and implementation of the strategy.

Source: Authors' own elaboration.

Table 2: Good practices from Member States on the deployment of the governance model

	Good Practices
Political governance	
1	Provide political support in the development and implementation of NCSS and governance models;
2	Ensure adequate coordination and cooperation among the relevant players;
3	Build trust between the different stakeholders;
4	Follow participatory approaches by putting in place platforms of exchange;
5	Involve all stakeholders in the process of developing an NCSS and a governance model (choose the right level of representation for the different stakeholders);
6	Set up a collaborative platform to monitor the progress of the action plan;
7	Ensure support from the highest political level in the creation of PPPs;
8	Mandate a single body to ensure the coordination and the implementation of the overall strategy;
9	Precisely define the roles and responsibilities of the different stakeholders involved in the governance model in one document;

Good Practices	
10	Create PPPs;
11	Ensure that the governance framework is supported by and defined by the legal framework.
12	Develop a section focused on the human rights in the NCSS and its governance model with explicit actions, responsibilities and roles
Strategic governance	
1	Develop a dedicated budget from bottom to top; particularly, allocate a dedicated budget for the cybersecurity strategy rather than allocating the budget to an overarching authority;
2	Include a paragraph on financials in the NCSS;
3	Thorough risk identification across different levels;
4	Early identification of risks and implementation of risk assessment mechanisms;
5	Follow a common methodology for risk identification;
6	Follow a common framework in case of incidents;
7	Definition of accountability and transparency rules;
8	Include legislation ensuring human rights in the NCSS.
Operational governance	
1	Tailored awareness-raising and training campaigns;
2	Centralise information sharing;
3	Taxonomy of best practices to ensure coherent processes of information sharing;
4	Formalise a coordinated approach between CSIRTs.
Technical governance	
1	Include in the NCSS and its governance model a section focused on international standards and technical guidelines. When developing this section, refer to the technical standards that should be used. The standards can be specified in another document to simplify their update. It is also important to define clear roles and responsibilities;
2	Have in place a body that supervises the compliance of regulated entities with national, European and international requirements.
3	Put in place in the NCSS action plan a group of tasks focused on using tools and technologies in respect to human rights, particularly to GDPR.

Source: Authors' own elaboration.

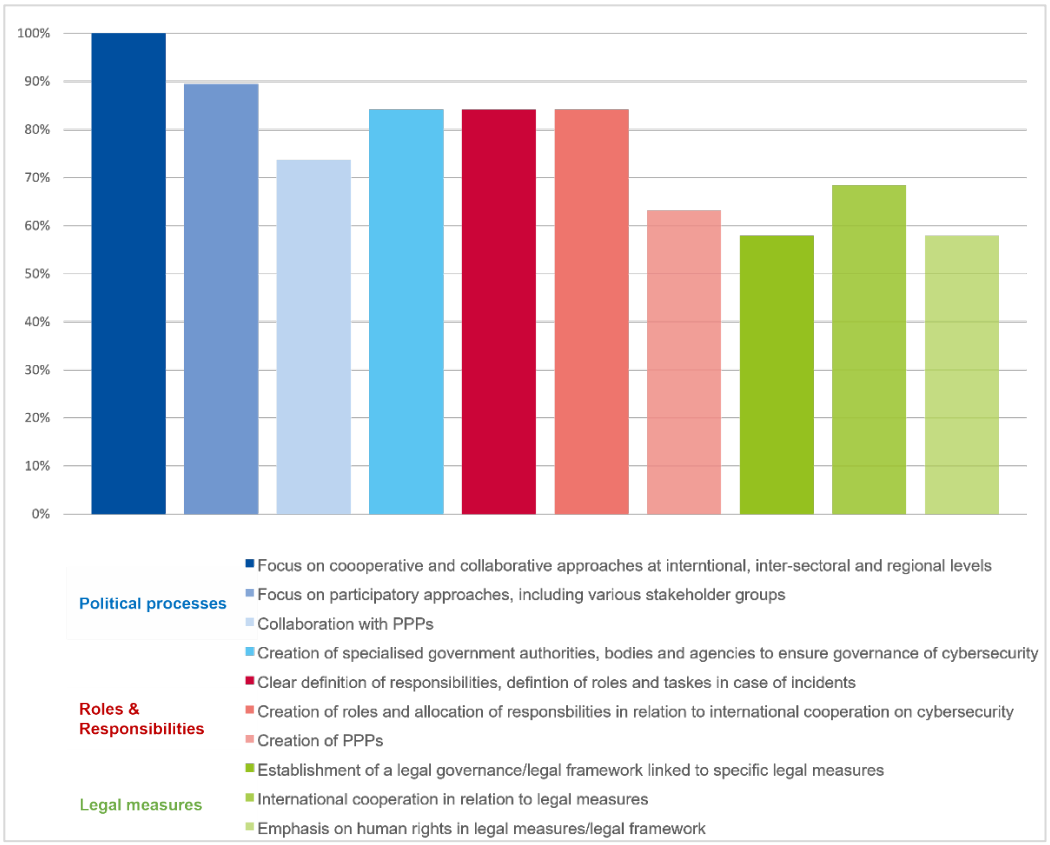
5.1 POLITICAL GOVERNANCE

The political governance level has been proven to build a highly important part of the governance model. All Member States' representatives indicated that political governance is

currently part of their governance model. It aims to clearly define political processes, identify and assign roles and responsibilities of different stakeholders, and put in place legal measures to support the deployment of the strategy.

Overall, three clusters of elements of political governance have been identified during the desk research. These have been further detailed and validated through stakeholder consultation. Figure 8 shows the percentage of stakeholders, interviewed in the process of this study, validating the element of political governance.

Figure 8: Percentage of interviewed stakeholders confirming elements of political governance



Source: Authors' own elaboration.

5.1.1 Political processes

Focus on cooperative and collaborative approaches at international, inter-sectoral and regional levels

An important element of the political governance is the inclusion of cooperative and collaborative approaches at international, inter-sectoral and regional levels. All the stakeholders interviewed confirmed that this element is already part the currently deployed governance model in their country.

The EU Member States follow different approaches to defining cooperative and collaborative aspects of political processes. Some Member States define those in the NCSS itself, while others detail them in the accompanying governance model or the legal framework.

At the national level, strategies focus more on the collaboration between governmental entities and across sectors.

GOOD PRACTICE

An international commitment and collaboration with international organisations and other countries is mentioned as a key objective of the strategy.

At the international level, most Member States cooperate to varying degrees with European institutions such as ENISA, Europol, etc. However, some Member States are interested in further developing this collaboration to also promote human rights, fundamental freedoms and democratic values in the cyber domain to ensure that it remains a global, open, stable and secure space, in which international law and shared principles are respected.

Main Observations

Providing political support: political authorities must take the cyber security topic seriously, get involved and support the development and implementation of its NCSS and governance models together with the other stakeholders. Governments should balance between facilitating and stimulating ownership and creating responsibilities for other stakeholders.

Ensure adequate coordination and cooperation among relevant players: a specific action plan for each of the relevant agencies should be developed, to define activities to be conducted about the strategic goals of the strategy.

Build trust between the different stakeholders: the most inclusive approach possible should be followed to collect inputs from the different parties involved. The level of participation in the decision-making process may vary according to the political setup of the country.

Follow participatory approaches by putting in place platforms of exchange where public sector entities, such as the government, its bodies and agencies are collaborating with NGOs, and stakeholders from the private sector but also from the scientific community and academia. This will facilitate cooperation across different actors from different domains to collect relevant insights.

Focus on participatory approaches, including various stakeholder groups

It is important to include other stakeholders such as academia, consultancies and other expert bodies, PPPs and representatives of critical infrastructures in the deploying of the NCSS. Participatory approaches have been identified as an important element of political governance and have been validated as such by most of the stakeholders interviewed. 89% of the interviewed Member States confirmed that this element is part of the currently employed governance model.

Main Observations

Involve all the stakeholders in the process of developing an NCSS and a governance model: Every institution, private company, and individual can positively contribute to the development of cyber security. Thus, at least the following stakeholders should be involved in the process:

- Government bodies and agencies;
- Private actors such as SMEs or private industry such as internet providers or telecom operations;
- Critical infrastructure operators;
- Law enforcement agencies;
- Scientific community; and
- Academia.

Hence, it is crucial to have an open dialogue through bilateral and multilateral discussions with all the relevant actors.

GOOD PRACTICE

In order to avoid duplications of efforts and overlapping mandates of the different agencies, a flexible decision - making process that allows for amendments should be put in place to provide for an agile process open to developments in the ecosystem.

Define a clear allocation of roles and responsibilities in the governance model: The definition of roles and responsibilities starts with the political decision on the level of representation for the different stakeholders, continues with the definition of allocation of roles and responsibilities and is finalised by the creation of a monitoring plan for each initiative to track the implementation of the actions. A clear allocation is fundamental to avoid the creation of overlaps of mandates among agencies and the creation of a mechanism that holds the different stakeholders accountable.

Set up of a collaboration platform: following the creation of a concrete action plan to implement the objectives of the strategy, the set up a collaborative platform is a powerful tool to monitor the level of implementation of the NCSS and to engage the different stakeholders regularly. Additionally, the platform can bring together the public and private sectors and foster the exchange of information.

Collaboration with PPPs

PPPs play an important role in the enforcement and accountability of political governance, they help support the inclusive approach in setting up the strategy and its governance model. This has been validated by most of the stakeholders interviewed: 13 of the 19 Member States' representatives interviewed confirmed that PPPs are currently employed in their actual governance model. For the 5 other Member States, PPPs are not explicitly mentioned in the strategy or governance model, but this it is highly encouraged by the country's authorities.

Depending on the sector, the Member States adopt a hybrid approach. In some instances, the collaboration is outsourced to independent PPPs, while in others, it takes place between government entities and PPPs.

The collaboration with the PPPs takes place between the government (different ministries) and the national bodies responsible for cybersecurity. Depending on the domain being discussed and the stakeholders involved, meetings are organised on a recurrent basis and can vary from a weekly to a monthly basis. The nature of the collaborative approach may change according to the topic being addressed.

GOOD PRACTICE

Deploy a web platform leveraged to collect, assess and evaluate the inputs entered by the private and public stakeholders and provide updates on the state of play of the strategy.

Main Observations

Support from the highest political level in the creation of PPPs: Interviews with Member State representatives highlighted the importance of public sector support and willingness to collaborate with the private sector due to the higher reactivity of the private one to the ever-changing cyber ecosystem.

GOOD PRACTICE

In the reporting phase for the implementation of the different initiatives of the NCSS, it is important to set up a framework that supports collaboration among stakeholders rather than competition. A good practice is to impose a simultaneal submission of the regular reports from the different stakeholders.

5.1.2 Roles and responsibilities

Creation of specialised government authorities, bodies and agencies to ensure governance of cybersecurity

The establishment of specialised government bodies to ensure the governance of cybersecurity has been identified as an important element of political governance. This has been validated by all the interviewed stakeholders, all of them have in place specialised government authorities, bodies, and agencies to ensure governance of cybersecurity.

The aim of the creation of a specialized body or agency in the cyber domain is to supervise, coordinate and monitor the deployment of the NCSS, and to ensure the coordination of the alignment of all the relevant stakeholders.

Depending on the country, the central body or agency responsible for cybersecurity can have different type of mandates and varying roles on the implementation of the NCSS. If in some countries as Estonia the cybersecurity centre is the main body overseeing the activities related to cybersecurity and sharing information with state authorities and private companies, in some other instances such as Denmark, the centre plays more a supportive rather than a governing role.

For those Member States that do not have a dedicated cybersecurity centre in place, an alternative committee is generally set up with the role of political coordination among parties.

Main Observations

Mandate a single body to ensure the coordination and the implementation of the overall strategy: this will allow to allocate specific roles, responsibilities, actions and follow the progress of the implementation.

Creation of roles and allocation of responsibilities related to national and international cooperation on cybersecurity

The definition of roles responsibilities related to international cooperation on cybersecurity has been identified as quite an important element of the political governance. This has been validated by almost all the interviewed stakeholders, in fact, 84% of them has defined in their governance model clear roles, responsibilities and task in case of incident.

Main Observations

Define in a very precise way roles and responsibilities of the different stakeholders: In the strategy, there should a dedicated section defining **the roles and responsibilities,** on the national as well as international level to avoid duplication of work and better monitor the implementation of the strategy.

Define the roles and responsibilities of the different stakeholders in the same document: it will allow to have an overview of the objectives, the tasks, and the stakeholders in charge of implementing them. Thus, it will help to better monitor the implementation of the strategy.

Creation of PPPs

Although not all the Member States interviewed (63%) currently have strong PPPs in place, it can be noticed that this aspect is very important and is increasingly encouraged by the different authorities.

Main Observations

Create PPPs: the creation of PPPs is a powerful tool supporting the development and deployment of the governance model. It permeates the strategy to strengthen the cyber resilience of the country and society. As cyberspace is composed of ICT products and services mainly produced or provided by private entities, the strategy should take into consideration close cooperation and continuous public-private consultation.

GOOD PRACTICES

International cooperation can be fostered through:

- Creation of a coordination group to liaise for the participation in the different international exchanges;
- Definition of working groups to interact with international organisations;
- Development of specific procedures for the allocation of responsibilities and roles related to international cooperation.

5.1.3 Legal measures

Establishment of a legal governance/legal framework linked to specific legal measures

The establishment of a legal governance/legal framework linked to specific legal measures has been identified as quite an important element of the political governance. 58% of the interviewed Member States have already in place a legal framework linked to specific legal measures.

In Europe, there is a common legal ground defined by legal acts as the NIS Directive, however, it is entrusted to each country the definition of a proper legal framework that supports the implementation of the strategy and the correct allocation of roles and responsibilities, as well as resources. Based on the interviews conducted, the definition of a legal framework is a sign of the maturity of the country, and it fosters the allocation of budget to the implantation of the NCSS, as well as the clear definition of mandates for the involved bodies. All these elements provide more stability and empower the governance model related to the NCSS.

Main Observations

The governance framework is supported by and defined by the legal framework: the legal framework is composed of newly introduced legal measures as well as already existing **legal measures whose scope has been enlarged to achieve the NCSS's objectives as well.**

International cooperation about legal measures

International cooperation about legal measures has been identified as quite an important element of political governance, as confirmed by 68% of the interviewed Member States.

First of all, it can be noticed that as members of the European Union, the interviewees are involved in different European and international initiatives on cybersecurity. The same applies to NATO member countries. For cooperation with non-European countries, MoUs (Memorandum of Understanding) are generally used.

Regional coalitions such as Greece, Cyprus and Israel can also be seen joining forces to enhance cooperation in the cyber security field.

Overall, an important part of the Member States strategies relates to the aspect that the actions should be mirroring general trends and activities on the EU-level in order to ensure the alignment with the EU trends.

Emphasis on human rights in legal measures/legal framework:

The emphasis on human rights in the digital sphere is not often covered by national legislation, except for very specific cases as GDPR. Similarly, this aspect is not often included in the Member States NCSSs. Nonetheless, many initiatives are taking place at European level (e.g., signing of the Berlin Declaration) given its recognised importance.

Main Observations

Develop a section focused on the human rights in the NCSS and its governance model with explicit actions, responsibilities and roles.

GOOD PRACTICE

Put in place a set of guidelines, certification schemes and sectorial policies addressed to public entities and private operators.

- the support for the development of European and international cybersecurity certification schemes and standards;
- the promotion of the inclusion of cybersecurity requisites in ICT procurement activities of Public Administrations.

5.2 STRATEGIC GOVERNANCE

Aiming at coordinating the processes of drafting the NCSS and setting up the accompanying governance model, strategic governance has been proven to build a highly important part of the governance model. All representatives indicated that strategic governance is currently part of the governance model employed in their country.

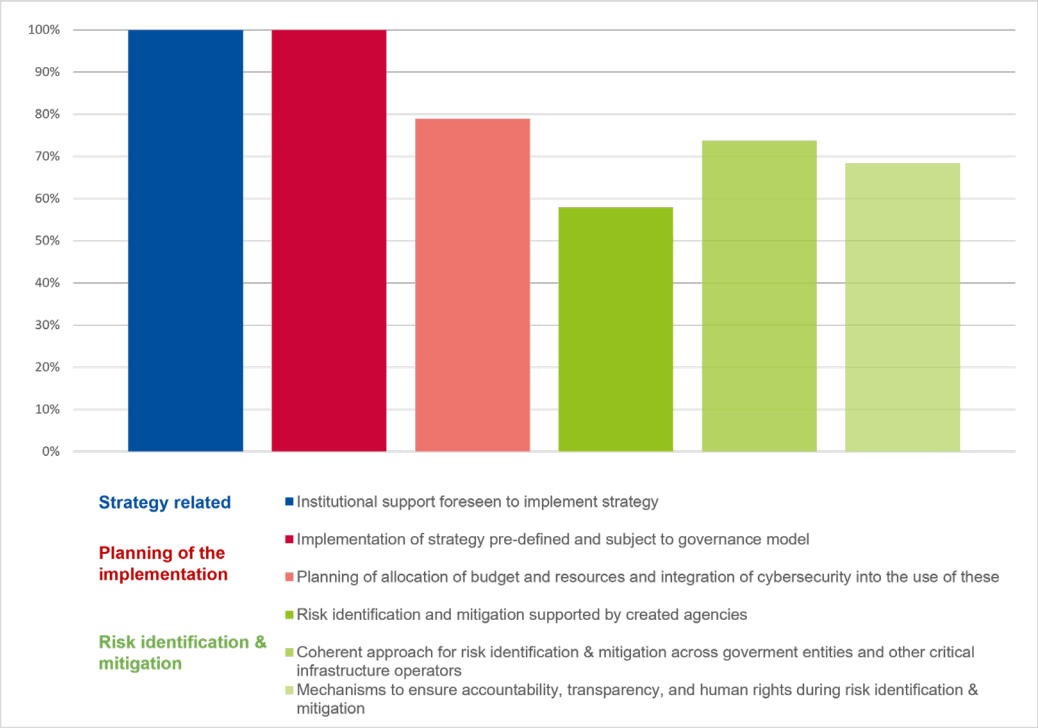
Overall, three clusters of elements of strategic governance have been identified during the desk research as pointed out in chapter 4. These have been further detailed on and validated through stakeholder consultation. Figure 9 here below indicates the percentage of interviewed stakeholders confirming the existence of the identified elements of strategic governance in their country's NCSS.

a) Elements concerning the NCSS itself
   - Foreseeing institutional support to implement the NCSS at the time of drafting the strategy;

b) Elements related to the planning of the implementation of the governance model and the strategy
   - Pre-defining a governance model to implement the NCSS, at the same time as drafting the NCSS;
   - Planning and allocation of budget and resources and integrating cybersecurity into the overall allocation thereof;

c) Elements of the strategic aspects of risk identification and mitigation.
   - Risk identification and mitigation supported by created agencies;
   - Coherent approach for risk identification and mitigation across government entities and other critical infrastructure operators;
   - Mechanisms to ensure accountability, transparency, and human rights during risk identification and mitigation.

Figure 9: Percentage of interviewed stakeholders confirming elements of strategic governance



Source: Authors' own elaboration.

As mentioned in chapter 4, the elements of strategic governance can be divided into two main groups, elements which should be taken into account from the beginning when developing the NCSS and elements that focus on the strategic aspects of risk identification and mitigation.

5.2.1 Elements concerning the NCSS itself

Foreseeing institutional support to implement the NCSS

The support of governmental entities or other public sector actors in implementing the NCSS has been identified as an important element of the strategic governance layer to ensure accountability of the strategy as well as support of a wider audience, triggered by wide political and institutional support across government entities. As presented in Figure 9 this has been validated by all stakeholders interviewed: all Member States' representatives interviewed confirmed that this element is part of the currently employed governance model.

The support of different governmental actors from the outset of developing the strategy is highly important to reach consensus and to define a coherent governance model accepted throughout all levels, ministries and sectors of government. While the governance model could be broken down, as the strategy, vertically and horizontally and be focussed on by different governmental actors, the overall NCSS should be agreed upon across the whole government and all involved institutions.

5.2.2 Elements related to the planning of the governance model and strategy's implementation

Pre-defining a governance model to implement the NCSS

This element of strategic governance aims to put the processes of drafting the NCSS and defining the governance model for the strategy's implementation in parallel. It has been proven most beneficial to adjust the timelines of both, the drafting of the strategy, and the planning of the governance model or accompanying action plan to be run at the same time. By doing so, no time is lost due to time lags between the drafting of the strategy and developing corresponding actions for its implementation.

All stakeholders interviewed mentioned that this element is entailed in the current governance model deployed. Additionally, it has been mentioned that while aligning the timelines was not always ensured, it will be ensured for future strategies as well, as it has proven to be more efficient for the implementation of the NCSS and to reach its objectives.

GOOD PRACTICE

Including detailed explanations of the foreseen implementation of the NCSS and references to the strategy itself in the action plan/ set-up of the governance model, while referencing the action plan/governance model in the NCSS.

Planning of allocation of budget and resources and integration of cybersecurity into the overall allocation thereof

The allocation of budget and resources to implement the NCSS is highly important, similarly is the planning of the allocation from an early stage of the development of the NCSS and its governance model. Thorough planning of the foreseen budget and resources is important to integrate the implementation of the NCSS specifically and cybersecurity in general into the overall national budget planning. Additionally, it is important to define general national priorities and to place the priorities of the NCSS within these to ensure alignment across all national priorities, budget and resource allocation and to properly integrate the NCSS and the governance model into the overall policy framework.

A majority (79%) of the interviewed stakeholders stated that the allocation of resources and budget is taken into account in the context of the NCSS and the accompanying governance model. However, it has been pointed out that while this planning is taken into account, it is rarely outlined in detail and most often performed separately from the definition of the NCSS and the development of the governance model. To some extent, this is driven by the political model employed by the states, i.e., the budget is mainly dealt with on the state level in federalism, and not on a national level; alternatively, budget allocation is done per ministry and hence, in a decentralised approach, if several ministries are accountable for different parts of the implementation of the NCSS. It has been stated that specifying a dedicated budget for the NCSS is recommended rather than allocating money to an overarching authority.

Main Observations

Developing the budget from bottom to top: Assign coordinators to each action, create an implementation plan per action and estimate the number of resources and budget needed to reach the defined objective. Afterwards, all budget estimates are aggregated and an overall estimate for the implementation of the NCSS is drafted, which is then included in the budget of the authority in charge as well as in the national budget.

Paragraph on financials in NCSS: The strategy itself includes a paragraph that identifying the country's investments in cybersecurity and defines an overall budget for the implementation of the NCSS and its objectives. The budget is divided per stakeholder/ministry in charge, rather than per objective.

5.2.3 Elements of the strategic aspects of risk identification and mitigation

Risk identification and mitigation supported by created agencies

Setting up a strategy for risk identification and mitigation is highly important in order to be prepared for cyber threats and attacks, to identify and mitigate them. Desk research has shown that a common practice is to create specialised agencies to support the implementation and operationalisation of this element of governance. A small majority (58%) of the interviewed stakeholders mentioned that this element is part of the currently deployed governance model of their country.

The creation of specific agencies providing services of risk identification and mitigation has been pointed out, as centralizing these aspects facilitates exchanges. It has been indicated that there seems to be a general lack of risk management if no dedicated agency is in place, but every critical infrastructure operator is responsible for risk identification and mitigation in their domain and this might create gaps or overlapping measures. Nevertheless, not creating dedicated authorities does not necessarily imply a lower level of efficiency in risk identification and mitigation, e.g., the national cybersecurity responsible agency could also be appointed the responsibility and lead the national activities.

Main Observations

Thorough risk identification across different levels: Agencies for identifying and mitigating risks are created at national level, these deal with the central government and critical entities. In addition, specific entities are created across the main sectors to cover risk identification and mitigation from a more domain specific angle, e.g., health, economic affairs, or climate. Lastly, leveraging on existing security and intelligence agencies, whose responsibilities have been extended to also cover cybersecurity aspects, could be a third option to build bodies responsible for risk identification. These three options could be used complementary or as stand-alone.

Early on identification of risks and implementation of risk assessment: Discussions to identify risks should take place during the process of drafting the NCSS already. The process includes stakeholders from the competent authorities, agencies and private sector as well as additional experts. The discussions should support on identifying potential risks, assessing the risks and developing measures to address these. The developed measures can be included in the NCSS or an accompanying action plan, highlighting responsible actors, identifying actions, and objectives.

Coherent approach for risk identification and mitigation across government entities and other critical infrastructure operators

Applying a coherent approach for risk identification and mitigation across the involved government entities and other involved critical infrastructure operators has been identified as important element of the strategic governance level. It facilitates exchange and information sharing in case needed and foster cooperation between the involved entities. The majority (74%) of country representatives interviewed, confirmed this and pointed out that although a coherent approach is difficult to implement, it is most often a clear goal of the NCSS.

While creating dedicated agencies for risk identification and mitigation facilitates the process, it includes the risk of separating processes and actors and each body leveraging its own approach. Hence, this might hamper collaboration, cooperation and communication, which are essentials for risk mitigation. Therefore, adopting a common and coherent approach is crucial.

Main Observations

Following a common methodology for risk identification: A document defining a common methodology for identifying risks should be developed early during the process of drafting the NCSS or when developing the governance model. Not differentiating between public and private actors, the document provides a solid methodological baseline for taking up a common approach for risk identification and mitigation across all involved actors.

Following a common framework in case of incidents: Some countries set-up a dedicated framework, which should be followed in case of incidents. The framework includes step-by-step processes for different actors in case of specific incidents or risks identified. The framework includes measures to be taken and also outlines dedicated comprehensive requirements which need to be undertaken in case of risk identification. This facilitates the uptake of a common approach across different actors.

GOOD PRACTICE

Daily communication: CERT bodies which are the main bodies responsible for the risk identification and mitigation communication on daily basis. In addition, working groups exchange opinions on an ad-hoc basis on specific issues, through defined communication channels.

Mechanisms to ensure accountability, transparency, and human rights during risk identification and mitigation

During risk identification and mitigation, accountability is a particularly important element to ensure that the objectives of a strategy will be achieved. Responsibilities are allocated and people need to be accountable for the actions to be taken in order to reach the objectives set out by the strategy. Setting-up mechanisms to ensure accountability of all actors involved is hence an important element of strategic governance to already ensure accountability from the set-out. Similarly, transparency is an important aspect during risk identification and mitigation, which needs to be ensured throughout all processes as to increase respect and acceptance by all players but also by the society as a whole. Developing mechanisms to ensure transparency has also been proven to be an important element of strategic governance. Last but not least, ensuring human rights in the digital sphere is particularly important in the context of cybersecurity and mechanisms need to be planned, developed and deployed to ensure human rights in general, and personal data protection in particular, while improving cybersecurity.

Discussing, developing and deploying these mechanisms for the NCSSs from an early point has been proven as important and the interviewed stakeholders confirmed this finding, as more than two-thirds (67%) of the interviewees stated that these mechanisms are at least partially in place in their country's governance model.

Main Observations

Definition of accountability and transparency rules: Rules and mechanisms to ensure accountability are clearly laid down in official documents, i.e., in the NCSS itself, its implementation/ action plan, and accompanying legal documents. Clearly defining the rules and mechanisms of accountability and transparency in the documents helps to ensure these aspects throughout the implementation.

Legislation ensuring human rights: Legislation on human rights is available in all Member States, nevertheless, additions and updates of existing and additional legal measures have been put in place to ensure human rights in the context of cybersecurity, in some Member States.

GOOD PRACTICE

Every institution in charge of implementing actions, policies, and projects under the NCSS is responsible to ensure accountability and transparency. The government of Lithuania then assesses from a strategic level how the agencies and institutions perform the actions according to pre-defined measures on accountability and transparency.

5.3 OPERATIONAL GOVERNANCE

Operational governance aims at operationalising the policies set out in the strategy to translate these into actions and improve cybersecurity across all layers of society. Specific elements of operational governance refer to:

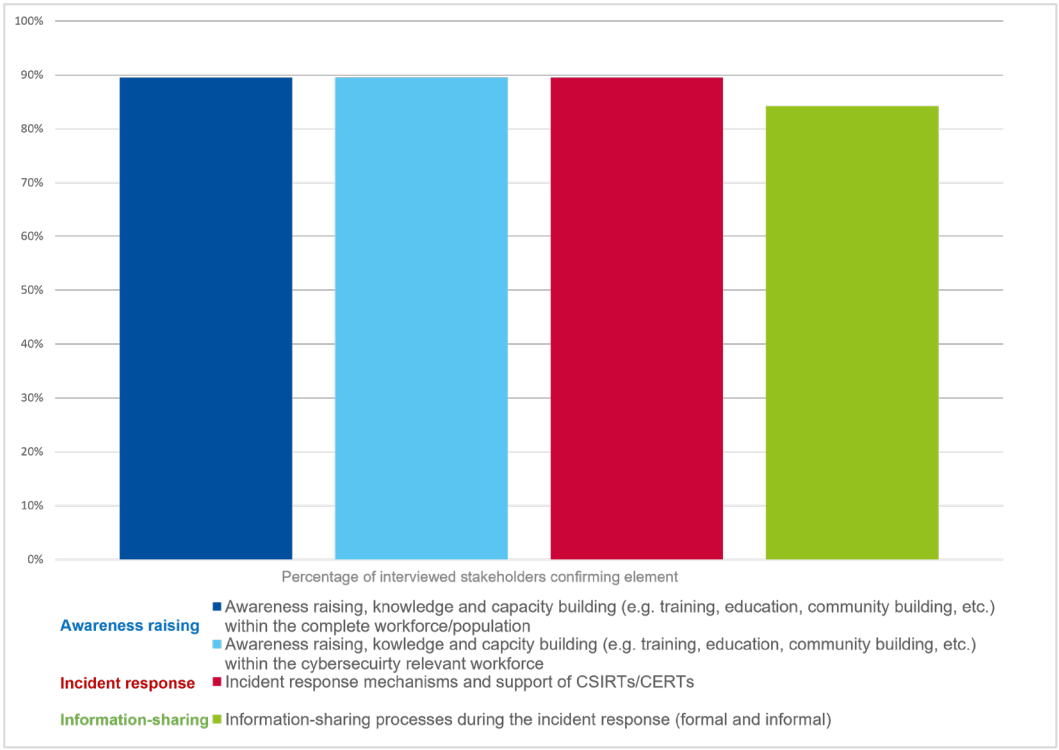
a) Elements about awareness-raising campaigns, outreach campaigns and training to foster capacity-building;
   - Awareness raising, knowledge and capacity building (e.g., training, education, community building, etc.) within the complete workforce/population;
   - Awareness raising, knowledge and capacity building (e.g., training, education, community building, etc.) within the cybersecurity-relevant workforce;

b) Elements about incident response;
   - Incident response mechanisms and support of CSIRTs and CERTs;

c) Elements about information-sharing processes and channels;
   - Informal and formal processes of information sharing during incident response;

All these elements have been validated by the stakeholders interviewed. 95% of the interviewed stakeholders confirmed that operational governance builds a part of their country's governance model. Similarly, all identified elements have been validated by a majority of the interviewed stakeholders, as deployed in Figure 10.

Figure 10: Percentage of interviewed stakeholders confirming elements of operational governance



Source: Authors' own elaboration.

5.3.1 Elements about awareness raising campaigns, outreach campaigns and trainings to foster capacity-building

Awareness-raising, knowledge and capacity building (e.g., training, education, community building, etc.) within the complete workforce/population

Raising awareness for cybersecurity across the whole workforce and/or the complete population is the main aim of many of the NCSSs of the Member States. It has been confirmed that a huge risk emerges from a population being unaware of cyber risks and being untrained on how to cope with these or how to safely behave in the cyberspace. Hence, training and education as well as awareness campaigns seem essential to increase the general level of knowledge and the general population's capacity about cybersecurity.

As depicted in Figure 10, 89% of the consulted countries pointed out that awareness-raising campaigns as well as educational campaigns targeting the overall population are already in place to increase the capacity of the general population and to increase their awareness of cyber risks. Nevertheless, while the importance of increasing awareness has been pointed out, it has also been stated that awareness raising comes with challenges and is a difficult topic to cover thoroughly.

Main Observations

Tailored awareness raising and training campaigns: Tailoring awareness raising and training campaigns to different stakeholder groups is important in order to account for the different needs and capabilities of the groups. Possible groups reflect businesses and other private sector entities, IT staff, cybersecurity specific staff, academia, and civilians.

GOOD PRACTICE

In 2018, Malta launched the nationwide cybersecurity awareness and education campaign. It targets different actors, from the private and public sectors, professionals, teens, the elderly, children, educators, vulnerable groups, public, etc.

Awareness raising, knowledge and capacity building (e.g., training, education, community building, etc.) within the cybersecurity relevant workforce.

It has been proven beneficial, to particularly raise awareness and knowledge on cyber, cyber threats and risks and cybersecurity among the people of the workforce which is most involved with and closely related to cybersecurity. Generally, the cybersecurity relevant workforce, most often has awareness of and skills in cybersecurity. However, cybersecurity being part of the quickly developing cyberspace necessitates constant training and education to keep up with changes, developments and new challenges. Additionally, it has been pointed out that there is a scarcity of skilled workforce in the cybersecurity domain, which implies that the workforce needs to be enlarged through policies aiming on training and education in the field of cybersecurity.

Similar to raising awareness and improving skills of the whole population, 89% of the consulted countries mentioned that this element constitutes an important part of their governance model. Awareness raising and training campaigns are covered to different extents by the countries' governance models. Some countries simply point out the importance and the objective to increase these aspects, while other countries are already more advanced, developing this element and provide concrete mechanisms, measures and actions in their governance model.

GOOD PRACTICE

MITA (Malta Information Technology Agency) was mandated with the role of a national coordination centre for training and awareness-raising. Currently, MITA is collaborating with the University of Malta and other stakeholders for the creation of masters specialised in cybersecurity for example.

5.3.2 Elements of the incident response

Incident response mechanisms and support of CSIRTs and CERTs

Formalised processes for incident response are a main element defined in the operational governance level. Established CSIRT and CERT bodies provide support in case of cybersecurity incidents and provide a centralised contact point at national level to coordinate and enable quick and systematic reactions to incidents. As specialised teams dedicated to developing and deploy mechanisms for cybersecurity in general and incident response in particular, CSIRT and CERT bodies build an incremental part of the operational governance in specific and the implementation and achievement of the NCSSs' objectives in general. While CSIRTs and CERTs provide support during incident response times, they can also play a proactive role preventing incidents from happening and supporting governments in building resilience against cyber threats.

89% of the interviewed countries confirmed the importance of CSIRT and CERT bodies for incident response (Figure 10). Further, they mentioned that incident response mechanisms are part of their country's governance model with CSIRTs and CERTs playing an important role in supporting and leading these mechanisms.

GOOD PRACTICE

Platform to submit, share and react to incidents: There are mechanisms for sharing technical information and for pushing e.g., early warnings, news, etc. Recently, an online platform has been set-up, where it is possible to receive compliance and risk information from critical information infrastructures. Additionally, incidents can be submitted on the platform. These are synced with national CSIRT processes. If there is an incident notification, an immediate technical response can be triggered.

5.3.3 Elements of the information sharing processes

Informal and formal processes of information sharing during incident response

Establishing processes of information sharing is highly important to ensure coordinated reactions during incident response times. Formal pre-defined and transparent processes as well as informal ones should be developed and deployed. While formal processes of information sharing often provide for and enhance accountability, informal ones might be more effective and efficient.

As shown in Figure 10, 89% of the consulted countries confirmed that informal and formal processes of information sharing are important and constitute an element of the operational governance level of their country's governance model.

Main Observations

Centralise information sharing. Activities to centralise and intensify information-sharing have been undertaken by several Member States.

Taxonomy of best practices to ensure coherent processes of information sharing. Spain developed a taxonomy based on existing best practices and is deploying it across organisations to ensure a coherent approach towards information-sharing.

5.4 TECHNICAL GOVERNANCE

The technical governance level has been proven to build a highly important part of the governance model due to its role in the identification and implementation of standards at a national or international level, and definition of technical mechanisms. All representatives indicated that technical governance is currently part of the governance model employed in their country. Specific elements of technical governance refer to:

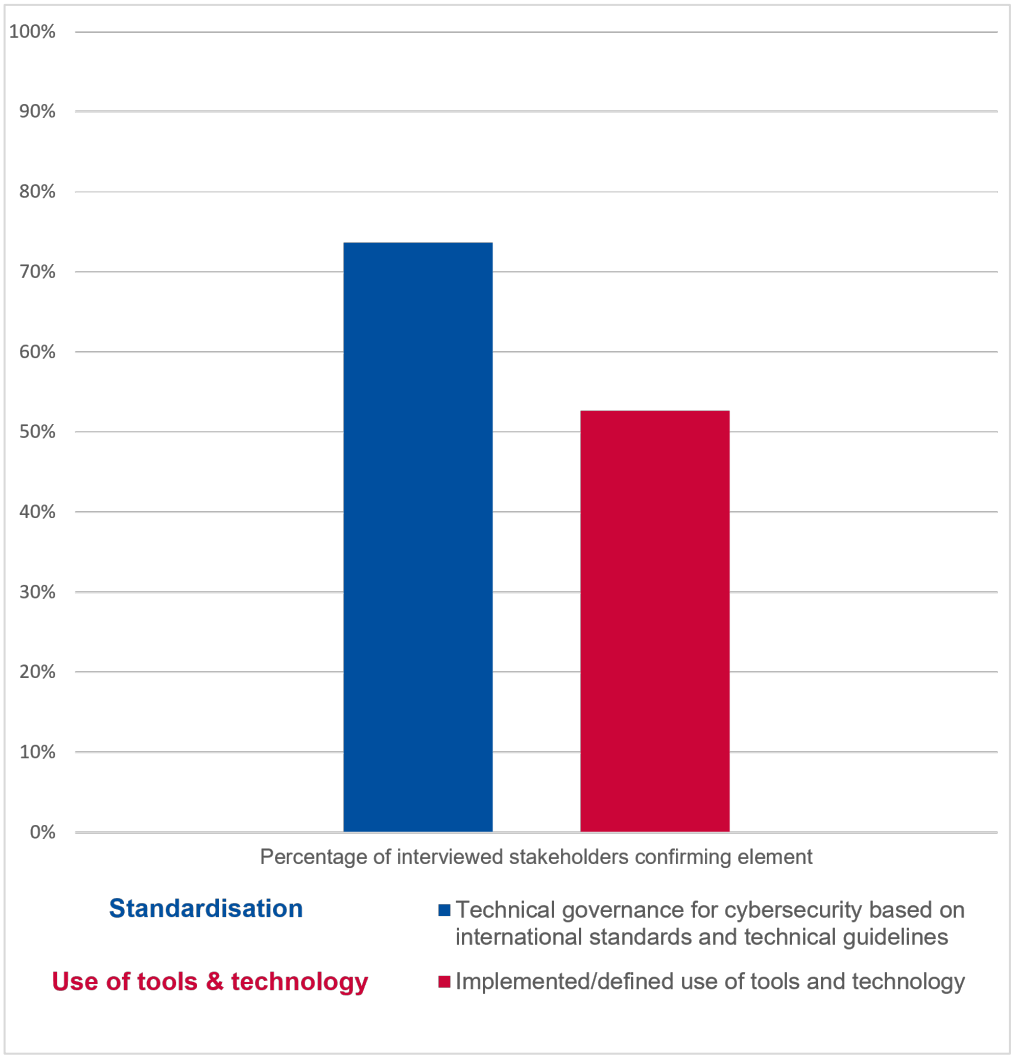
- Technical governance for cybersecurity based on international standards and technical guidelines; and
- Implemented/defined use of tools and technology.

GOOD PRACTICES

In Malta, a project has been started to create a specific team for information sharing called the "cyber threat intelligence team". The goal is to collect cyber threat intelligence from partners and share information.

In the Netherlands, survey has been started to examine the possibilities and modalities (legal, financial, etc.) to develop a public-private cooperation platform to strengthen situational awareness and the timely sharing of cyber threat information and advisories. The goal is to offer more information and a swifter perspective for action with relevant organisations. When doing so, attention is also paid to cybersecurity requirements and the level of maturity of the recipients of relevant information. This survey is a follow-up of the existing cyber intel/info cell, a public cooperation platform of operational public organisations (NCSC, Police, Intelligence and Security Services and Public Prosecutor), where information on cyber threats and cyber incidents is brought together and is jointly assessed by those organisations.

Figure 11: Percentage of interviewed stakeholders confirming elements of technical governance



Source: Authors' own elaboration.

5.4.1 Technological standardisation

Technical governance for cybersecurity based on international standards and technical guidelines

The technical governance for cybersecurity based on international standards and technical guidelines has been identified as an important element of the technical governance. 74% of the interviewed Member States take this into account in their strategies (Figure 11).

While this aspect is not addressed in all NCSS or is not very detailed, according to interviews with Member State representatives, this aspect is considered important.

The use of technical standards is mentioned in the strategy; however, it is not specified which technical standards should be used.

Main Observations

Include in the NCSS and its governance model a section focused on the international standards and technical guidelines: this will ensure to be aligned with the other Member States. When developing this section, specify which technical standards should be used,

and define clear roles and responsibilities. To simplify the update of standards, the standards could be described in a document accompanying the NCSS and the governance model. A key enabler is the existence of a body that supervises the compliance of regulated entities with the European and international requirements.

5.4.2 Use of technology, tools and certification schemes

Implemented/defined use of tools, technology and certification schemes

The importance of the use of cybersecurity certification schemes as a tool to manage risk is highlighted by European agencies and will be enforced under the NIS2 directive. European cybersecurity certification schemes should apply to the majority of ICT products and services, and in particular, to all the services or activities provided by essential entities. The competent authorities should be empowered to apply sanctions consisting of the suspension of a certification or authorisation concerning part or all the services provided by an essential entity.

Member States should establish a strategy to produce certificates for ICT solutions, either based on existing national schemes or next to come EU schemes, ensuring an ecosystem that can deliver certified solutions or participate to the certification of solutions through public or private conformity assessment bodies. Finally, their procurement policy or any implementation of national and/or EU laws should be based through the use of certified solutions.

The use of tools and technologies was highlighted as an important element in implementing NCSSs, although this point is not developed in the strategies of some countries. Nine out of the 18 interviewed Member States take this into account in their strategies, and 53% of all interviewed stakeholders validated this element of technical governance, as shown in Figure 11.

The representatives of the Member States interviewed stressed the importance of not only focusing on available standards but also taking into account improvements in technical security, based on the use of modern approaches to cybersecurity for the detection and handling of incidents. Threats and incidents are ever-evolving and hence, the instruments of cybersecurity to combat them need to quickly adapt.

Main Observations

Put in place in the NCSS action plan a group of tasks focused on using tools and technologies in respect to human rights, particularly to GDPR.

6. MONITORING A GOVERNANCE MODEL

Monitoring the governance model is an important factor to ensure the successful deployment of the governance model as well as for the successful implementation of the NCSS. Aiming to assess the effective implementation, monitoring mechanisms are hence highly important for the deployment of a governance model. Additionally, the use of an assessment framework can strengthen the accountability of the responsible stakeholders, foster progress in the deployment phase and provide insights for areas of improvements.

Monitoring mechanisms can take different forms and levels of detail and granularity. For instance, a traffic light system could be employed to indicate whether the progress of implementation is on track (green), behind schedule (yellow) or at risk (red). Traffic light systems provide broader and more qualitative information on the progress. A more granular approach of establishing monitoring mechanisms includes the development of Key Performance Indicators (KPIs). KPIs are measurable values, in the context of governance models, they provide quantifiable information on the progress of the implementation of actions, policies, and rules. KPIs could be of both quantitative as well as qualitative nature.

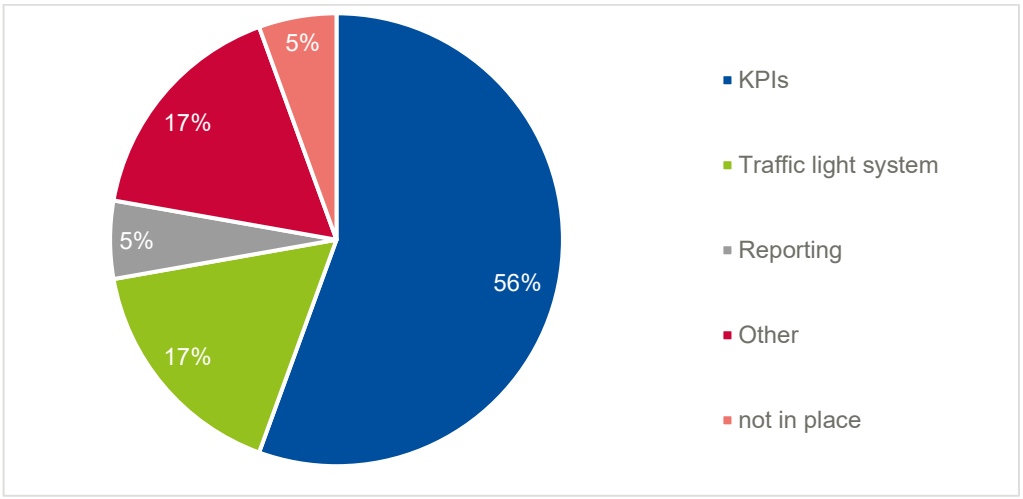
Another monitoring instrument used to evaluate the progress of the implementation of the governance model is reporting. This implies that accountable and responsible persons report on the progress of their specific actions to a higher-level authority. Reporting provides a more general overview of the progress and information are normally not quantifiable.

It has to be mentioned that other forms of monitoring could be deployed that are completer and more fit for purpose. However, the interviews highlighted that the Member States prefer light assessment methodologies. The remainder of this section will provide an overview of the deployment of monitoring mechanisms for evaluating the progress of the implementation of the governance models accompanying the NCSSs across the EU Member States.

6.1 MONITORING MECHANISMS OF GOVERNANCE MODELS DEPLOYED ACROSS THE MEMBER STATES

Figure 12 here below provides an overview of the adoption of monitoring mechanisms for the governance model across the interviewed countries. 17 out of the 18 consulted countries have some sort of monitoring mechanism in place, the majority (56%) already developed quantitative, and/or qualitative Key Performance Indicators. 17 % of the interviewed countries indicated that a traffic light system or another monitoring mechanism is in place to monitor and evaluate the progress of implementing the governance model and the NCSS. 5% of the interviewed countries mentioned that the evaluation of the progress of the implementation is based on reporting, provided by the accountable or responsible persons, per action or objective.

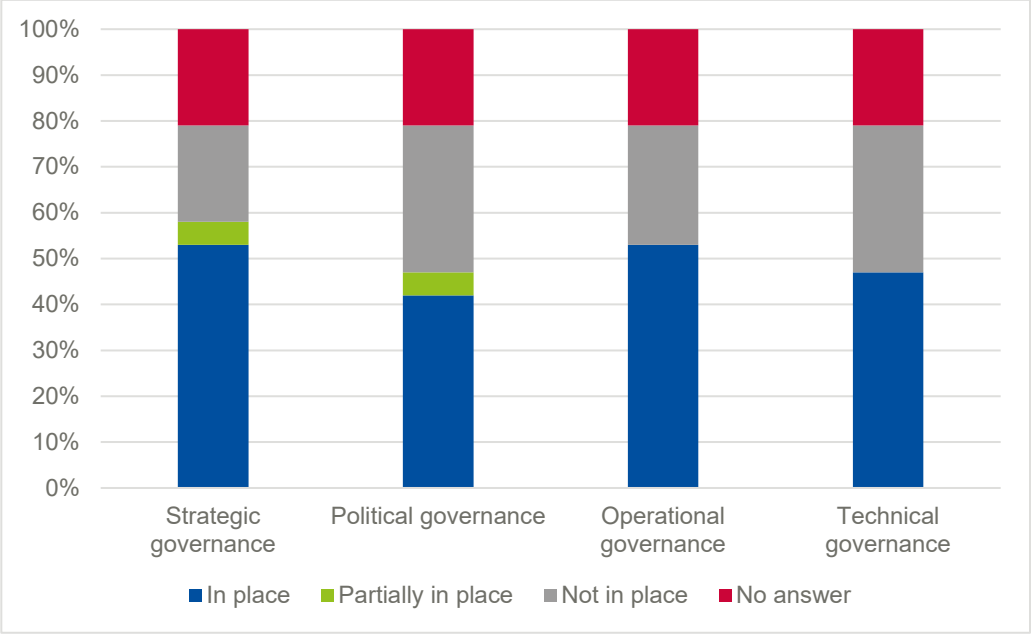
Figure 12: Deployment of monitoring mechanisms across the interviewed EU Member States



Source: Authors' own elaboration.

Figure 13 provides a more granular view of the implementation of monitoring mechanisms per governance level. It emerges from the stakeholder consultation that the majority of countries has monitoring mechanisms in place for the strategic and operational governance levels. 58% of the interviewed countries have a partially or completely deployed monitoring mechanism to evaluate the progress of implementing the NCSS from a strategic governance point of view. 53% employed monitoring mechanisms on the operational governance level, while progress on deploying the technical level of governance is systematically monitored in 47% of the countries. The same percentage of countries deployed monitoring mechanisms for the political governance level.

Figure 13: Monitoring mechanisms in place per level of governance



Source: Authors' own elaboration.

Generally, most countries monitor the progress by focusing on objectives or actions without creating a comprehensive assessment framework that could provide an overall index of progress.

Good practices in the context of establishing monitoring mechanisms have been identified from the interviews with the Member States' representatives. These are detailed here below.

Good Practice – Extended set of KPIs to also monitor the state of cybersecurity across the population

In **Spain** not only a set of KPIs has been established to monitor the progress of the implementation of the governance model, but a specific national observatory for cyber has been put in place. The observatory's main function is to monitor the KPIs and to publish reports on the KPIs deployed to measure the progress of the implementation.

In addition, the KPIs developed by Spain do not only cover the implementation of the governance model and the NCSS, but also aim at the wider objective of ensuring service and cybersecurity in the country. Therefore, additional KPIs have been introduced, which focus on the behaviour of citizens during incidents.

Many of the KPIs are publicly available to also provide the population with the possibility to inform themselves about the current status of the country, the goals and the progress. Furthermore, more sensitive KPIs, focusing on more policy-specific aspects have been established. These however are not publicly available to ensure security.

In Italy, it is foreseen develop specific measures and KPIs within the first twelve months after the adoption of the NCSS. The KPIs deployed will not only aim on measuring the progress of the implementation of the governance model and the NCSS, but some KPIs will aim at a more granular and more encompassing system to also measure:

- Cybersecurity maturity;
- Involvement of specific categories of persons (women, young, unemployed and jobseekers) in the cybersecurity training;
- Involvement of specific categories of persons (women, young, unemployed and jobseekers) in the cybersecurity industry;
- Cybersecurity investments;
    - Investments in and initiatives on cybersecurity research and development;
- **Number of national companies insured by cybersecurity incidents.**

Good Practice – Platform to enable the exchange of progress

In **Austria**, the new NCSS is not only set up to follow a whole-of-nation/whole-of-society approach but also to allow to react to changing challenges and opportunities in the cyberspace. Accompanying the NCSS, a web platform has been developed to collect and monitor objectives, and actions and to measure progress dynamically. By using the PPPP-Model also non-governmental stakeholders are allowed to add to the platform facilitating information sharing and exchange.

It provides insights into the progress of the implementation of the NCSS and its governance model. KPIs are developed to monitor the progress of reaching the strategic objectives and to implement the related measures. For every action, policy or measure of the governance model and the NCSS, a scorecard is created, each scorecard provides insights into the progress of the specific objective, action or measure. The monitoring on the scorecards is based on key project management principles in order to ensure granular and detailed monitoring of the progress.

Twice a year a report based on the data on the platform is created and published on the website of the Austrian Federal Chancellery thus giving the public insights into the state of play of Austrian Cybersecurity.

6.2 POTENTIAL RE-USE OF EXISTING KPIS

KPIs related to cybersecurity have been developed by different organisations already. The uptake of these indicators is encouraged, while some adjustment could be beneficial. Here

below a short explanation of three sets of KPIs related to cybersecurity is provided. The longlists of the KPIs deployed by the three sets are provided in the Annex of this report.

6.2.1 NCAF KPIs

The national capabilities self-assessment framework (NCAF), developed by ENISA, aims at measuring the level of maturity of the different NCSSs. The framework specifically should empower the Member States in

- Conducting the evaluation of their national cybersecurity capabilities.
- Enhancing awareness of the country's maturity level;
- Identifying areas for improvement; and
- Building cybersecurity capabilities.

The framework provides an assessment of the NCSSs on 17 objectives, grouped into four main clusters across five levels of maturity. The four main clusters of objectives are the following:

1. Cybersecurity governance and standards;
2. Capacity-building and awareness;
3. Legal and regulatory; and
4. Cooperation.

Among the different elements assessed to identify the level of maturity, there are some that refer to the governance model of an NCSS and can be extracted and reused to evaluate the governance model of a country. The specific indicators are listed in Annex B.1 of this report.

6.2.2 EU Cybersecurity Index

ENISA is working since 2021 on the development of an EU Cybersecurity Index, a tool to help Member States making informed decisions by providing insights on the cybersecurity maturity and posture of the Union and MS policies, capabilities and operations. With a view to the tasks included in the latest NIS 2 Directive Proposal text[59], the EU Cybersecurity Index project of ENISA is expected to evolve in the direction of a biennial report on the state of cybersecurity in the Union. For this aim, a set of indicators is being defined which will provide a better understanding on which areas the EU will need to focus on to improve the overall Union cybersecurity.

The development of the EU Cybersecurity Index is still work in progress and under consultation and piloting with the Member States' National Authorities. Currently, the focus and indicators of the index will provide a better understanding on which areas the EU will need to focus on to improve the overall Union cybersecurity. As soon as the NIS2 Directive has been finalised, work will commence to evolve from the EU Cybersecurity Index project of ENISA to the new requirements defined in the NIS 2 Directive and in particular Art. 15.

The main objectives of EU's Cybersecurity Index include:

- assessing the current level of maturity of cybersecurity and relevant cyber capabilities;
- identifying opportunities for collaborative and local cybersecurity enhancements; and
- identifying areas of network and information system security weaknesses which may provide a risk to the Union and its MS as well as its citizens, governmental structures, CI/CII and digital services, and small, medium, and large enterprises.

[59] Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148

For the time being the EU Cybersecurity Index consists of 58[60] composite indicators in four areas:

- Policy;
- Operations;
- Capacity; and
- Market/industry

The indicators are not yet publicly available but will be in due time.

6.2.3 ITU Global Cybersecurity Index indicators

The International Telecommunication Union (ITU) is the UN agency dedicated to ICTs and launched the Global Cybersecurity Index (GCI) to measure the commitment to cybersecurity of the countries around the globe. Aiming to assist the countries to identify possible areas of improvement related to cybersecurity, the GCI's main objective is to measure:

- The type, level, and evolution over time of cybersecurity commitment within countries and relative to other countries;
- The progress in cybersecurity commitment of countries from a global perspective;
- The progress in cybersecurity commitment from a regional perspective; and
- The cybersecurity commitment divide (i.e., the difference between countries in terms of their level of engagement in cybersecurity initiatives).

The 2020 GCI consists of 82 questions feeding into 20 indicators, which are mapped across five main pillars. The main pillars of the GCI are:

1. Legal measures;
2. Technical measures;
3. Organizational measures;
4. Capacity development measures; and
5. Cooperation measures.

All indicators are listed in Annex B.2 of this report. Under pillar 3, the organizational measures, the main indicator refers to the development, implementation and deployment of a national cybersecurity strategy. The specific questions feeding into this indicator are also listed in Annex B.2 of this report.

6.2.4 Cybersecurity Capacity Maturity Model for Nations (CMM)

Developed by the Global Cyber Security Capacity Centre[61], the goal of the Cybersecurity Capacity Maturity Model for Nations (CMM) is to increase the scale and effectiveness of cybersecurity capacity-building. A first version of the model was deployed in 2014 and a revised version has been made available in 2016 and a new one in 2021.

The CMM assesses cybersecurity capacity across five key dimensions, which – according to the model – represent the clusters of cybersecurity. The five dimensions are:

1. Developing cybersecurity policy and strategy;
2. Encouraging responsible cybersecurity culture within society;
3. Building cybersecurity knowledge and capabilities;
4. Creating effective legal and regulatory frameworks; and
5. Controlling risks through standards and technologies.

[60] Subject to review. The number of indicators might change based on consultations with cybersecurity experts coming from national authorities, EU Agencies, and the industry.
[61] The Global Cyber Security Capacity Centre is part of the Oxford Martin School within the University of Oxford.

The CMM is based on five maturity levels to evaluate a nation's level of capacity and to measure progress in relation to specific factors and/or aspects of cybersecurity capacity: Start-up; Formative; Established; Strategic; and Dynamic.[62]

The detail of each factor of the different dimensions are listed in Annex B.3 of this report.

[62] ENISA, National Capabilities Assessment Framework, 2020 ; Available at: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework.

7. CONCLUSION

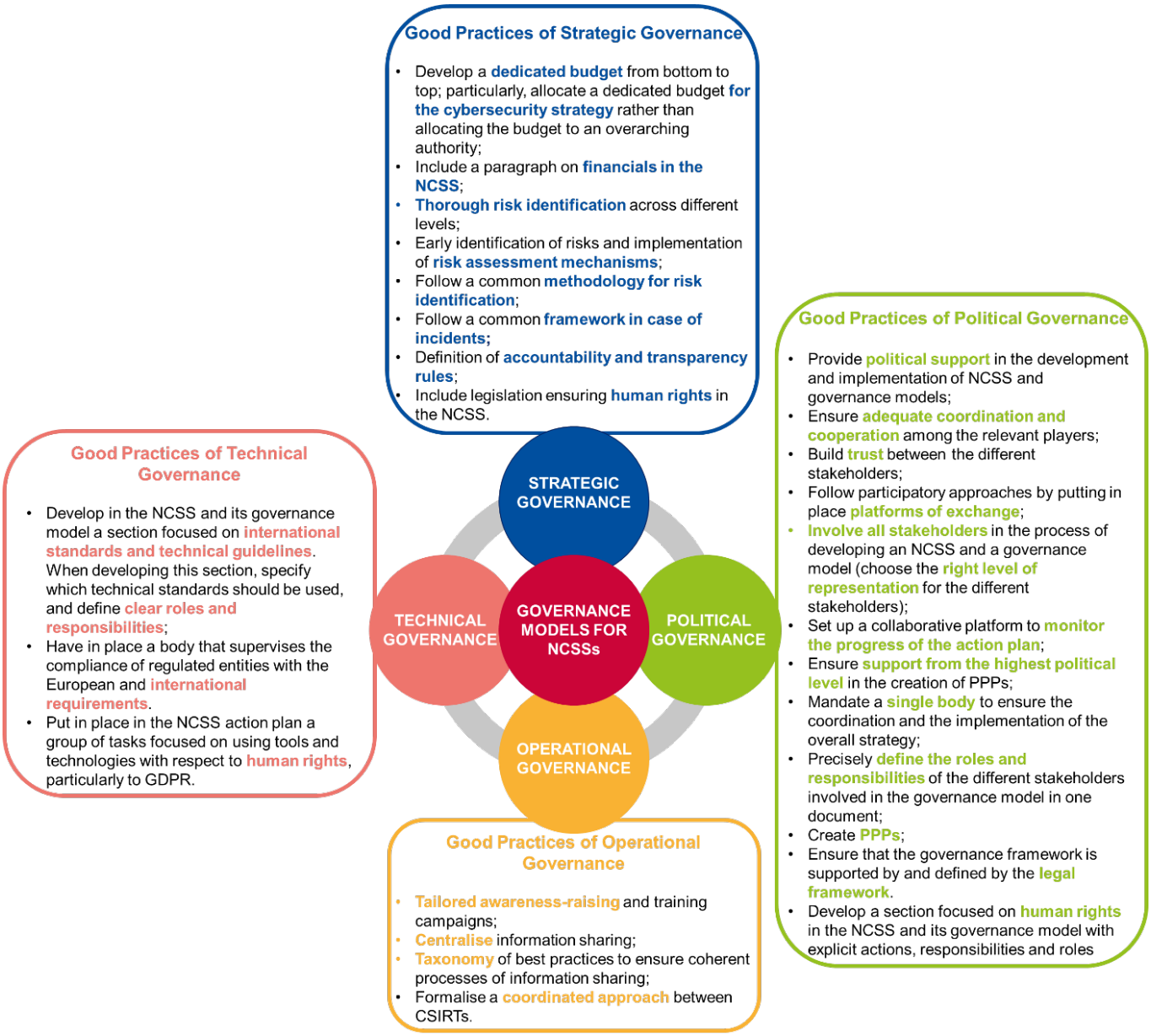
Aimed at developing a good practice example of effective governance models for NCSSs, different governance frameworks across the EU and beyond have been analysed. Based on desk research of more than 49 sources, and 19 interviews with representatives of the EU Member States, the analysis of the Governance Framework for NCSS from March to July 2022 resulted in some conclusions that can be regarded as takeaways for the Member States.

Identified through desk research, four main levels of governance frameworks have been identified as predominant. Specifically, these levels are:

1. Political governance;
2. Strategic governance;
3. Operational governance; and
4. Technical governance.

This study's research indicated that no evident correlation between the type of government, self-governance, and the governance model of the NCSS deployed exists. Rather, several additional factors such as the size of a country, its level of maturity in the cyber domain, and the level of cooperation with the private sector, influence the definition of a governance model. This finding led to the conclusion that it is not possible to have a unique governance model to be used as a reference. Therefore, good practices rather than a single best practice governance model have been identified for each layer. The four main levels of a governance framework have been further defined and sub-areas have been detailed through intensified desk research and interviews. These encompass all elements of good practice governance models.

Figure 14: Good Practices of governance model elements



Source: Authors' own elaboration.

In addition to the main elements governing the different levels of governance, the establishment of monitoring mechanisms, Key Performance Indicators (KPIs) and other measures to coherently monitor and evaluate progress, have been identified as important. KPIs and monitoring measures facilitate the finetuning of the strategy's actions and the successful implementation of the NCSSs and the related governance model.

With regard to KPIs, this study provides a list of KPIs already developed by different organisations, which could be adapted to the situation in different Member States.

8. BIBLIOGRAPHY / REFERENCES

Butcher, J., (1975). Copy-editing: The Cambridge handbook, Cambridge University Press, Cambridge.

Council of Europe, (2001). Impact of the European Convention on Human Rights – Budapest Convention, Council of Europe Portal, available https://www.coe.int/en/web/impact-convention-human-rights/convention-on-cybercrime#/.

Cybersecurity & Infrastructure Security Agency (CISA), (2017). Cybersecurity Governance Publications, CISA Publications, available https://www.cisa.gov/publication/cybersecurity-governance-publications.

Cybersecurity foundation, (2021). The NCS Guide 2021, available https://ncsguide.org/the-guide/.

European Communities, (1990). Economic transformation in Hungary and Poland, European Economy No 43, Office for Official Publications of the European Communities, Luxembourg, pp. 151-167.

Efe, A. & Bensghir, K. T., (2019) cited in Savas S. & Karatas, S. (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, 2022, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

ENISA, (2020). National Capabilities Assessment Framework, ENISA Publications, available at: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework.

ENISA, (2012). National Cyber Security Strategies: An Implementation Guide, ENISA Publications, available https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide.

ENISA, (2016). NCSS Good Practice Guide, ENISA Publications, available https://www.enisa.europa.eu/publications/ncss-good-practice-guide.

ENISA, (2018). Public-Private Partnerships (PPP) – Cooperative models, ENISA publications, available https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models.

ENISA, (2014). Threat Landscape report, European Union Agency for Network and Information Security.

European Parliament and Council, (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union – NIS Directive, EUR-Lex, available https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

European Parliament and Council, (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) – EU Cybersecurity Act, EUR-Lex, available https://eur-lex.europa.eu/eli/reg/2019/881/oj.

Hamm, E., (1980). Return of the English breakfast, International Cuisine, Vol. X, No 1, Unwin, London.

ISO, (2015). ISO/IEC 38599:2015 Information technology – Governance of IT for the organization, available https://www.iso.org/standard/62816.html.

ITU, (2021). Global Cybersecurity Index, ITU Publications, available https://www.itu.int/pub/D-STR-GCI.01-2021.

Marsh & McLennan, (2021). MMC Cyber Handbook 2021 – Cyber Resilience Perspectives: Clarity in the midst of Crisis, MarshMcLennan Publications, available https://www.marshmclennan.com/insights/publications/2020/october/mmc-cyber-handbook-2021-.html.

NIST, (2022). Computer Security Resource Center, Glossary, last updated 2022, available https://csrc.nist.gov/glossary.

NIST, (2020a) Success Stories – Israel National Cyber Directorate v. 1.0, available https://www.nist.gov/cyberframework/success-stories/israel-national-cyber-directorate-version-20.

NIST, (2020b). Success Stories – Japanese Cross-Sector Forum, available https://www.nist.gov/cyberframework/success-stories/japanese-cross-sector-forum.

NIST, (2018). Cybersecurity Framework, NIST Publications, 2018, available, https://www.nist.gov/cyberframework/resources.

Savas, S. & Karatas, S., (2022). Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity, International Cybersecurity Law Review, 3:7, available https://link.springer.com/article/10.1365/s43439-021-00045-4.

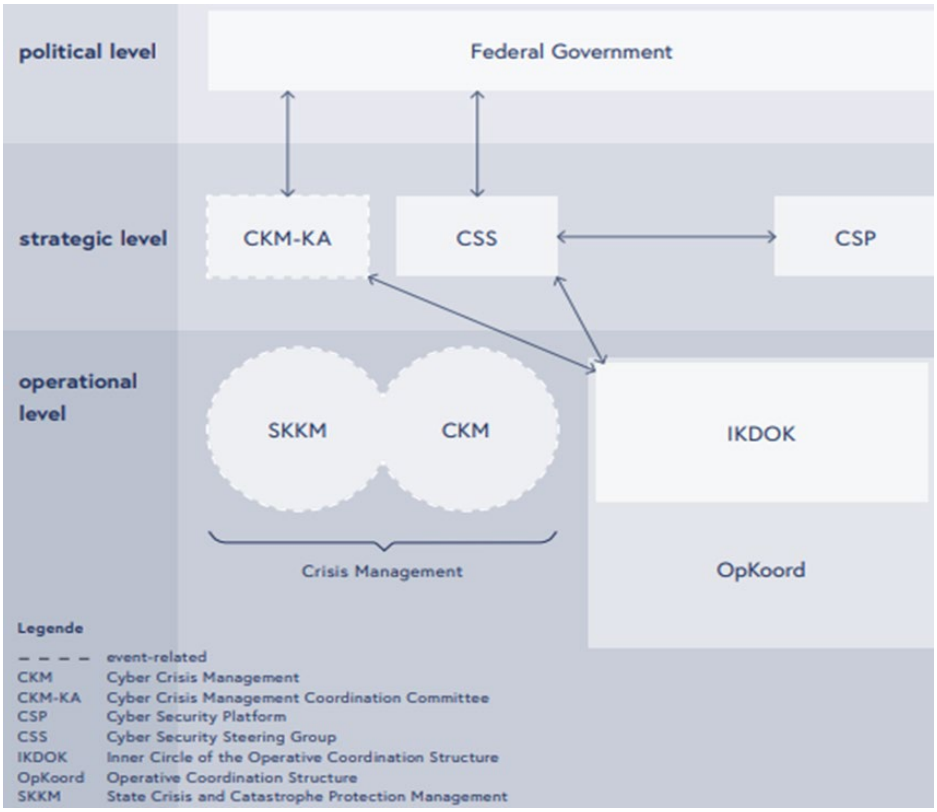
Sutherland, E., (2018). Cybersecurity: Governance of a New Technology, in: Proceedings of the PSA18 Political Studies Association International Conference, Cardiff, 26-28 March 2018, available https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3148970.

UK Cabinet Office, (2022). Government Cyber Security Strategy: 2022 to 2030, policy paper published by the UK Government, available https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030.

A ANNEX: ORGANISATIONAL CHARTS OF MEMBER STATES CYBERSECURITY ENTITIES

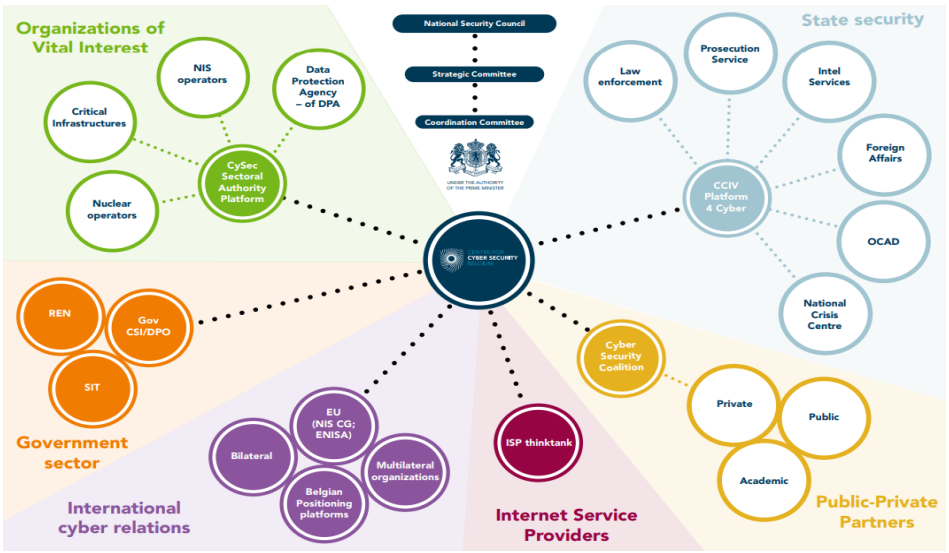
This Annex provides and overview of the different organisational charts of the Member States' political set-up for cybersecurity. Each organisational chart indicates the different levels and stakeholders involved in cybersecurity policies of the country and particularly in setting up the governance model for the NCSS.

A.1 AUSTRIA



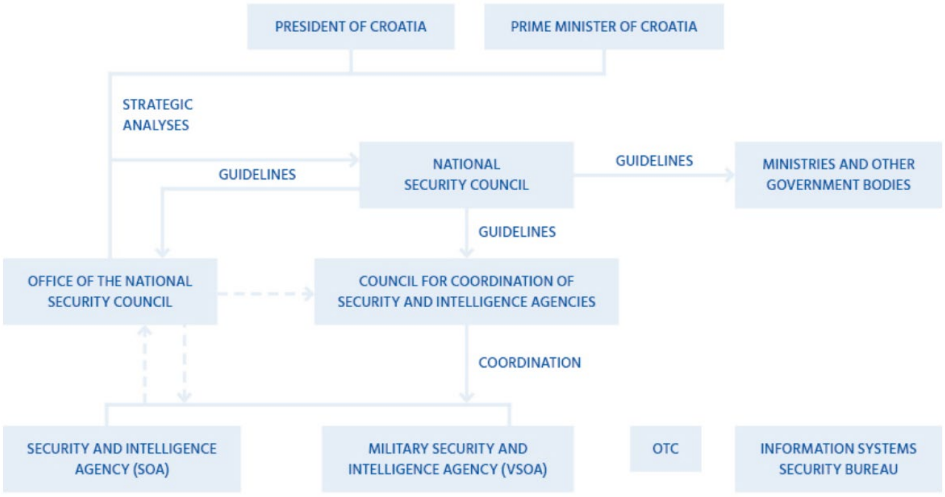
Source: Austrian Cybersecurity Strategy, 2021.

A.2 BELGIUM



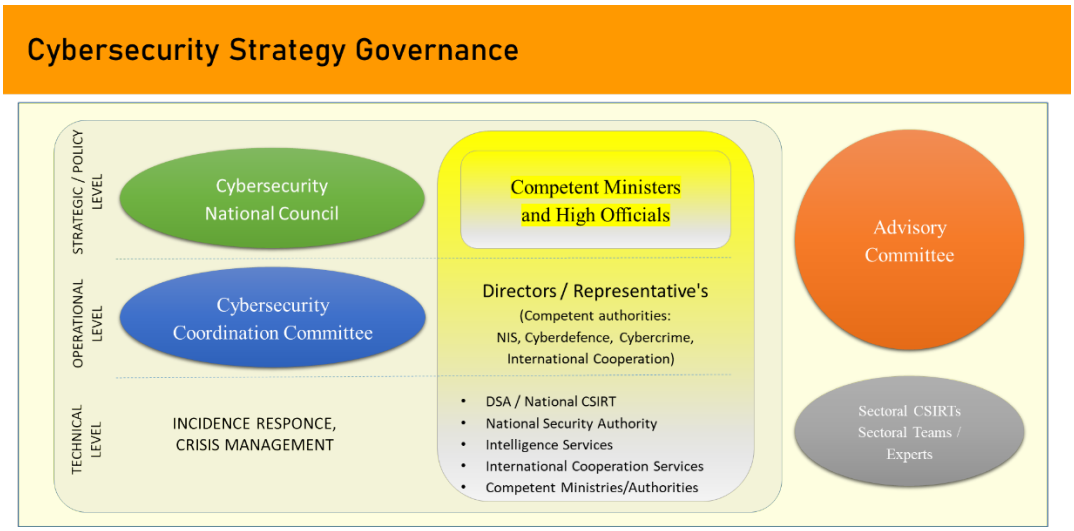
Source: Cyber security strategy Belgium, 2021.

A.3 CROATIA



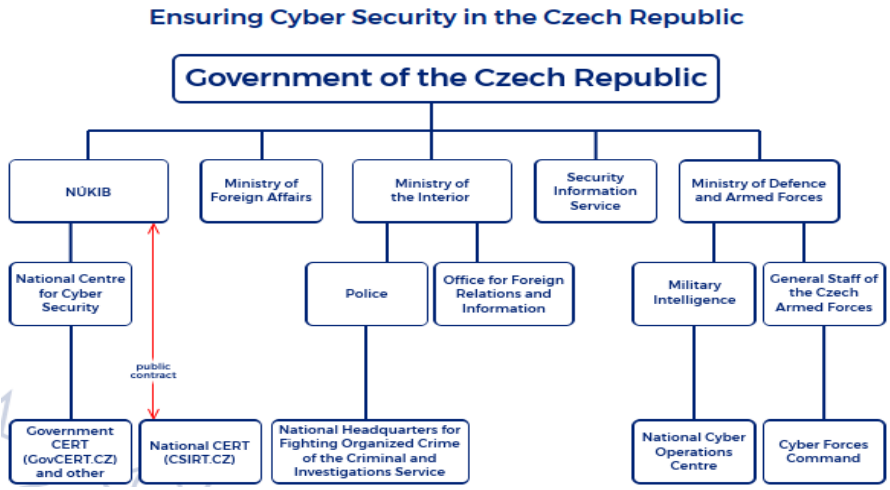
Source: Security Intelligence system of the Republic of Croatia, 2022.

A.4 CYPRUS



Source: Greek cybersecurity strategy, 2020.

A.5 CZECH REPUBLIC



Source: National Cyber Security Strategy of the Czech Republic 2021 – 2025.

A.6 ESTONIA

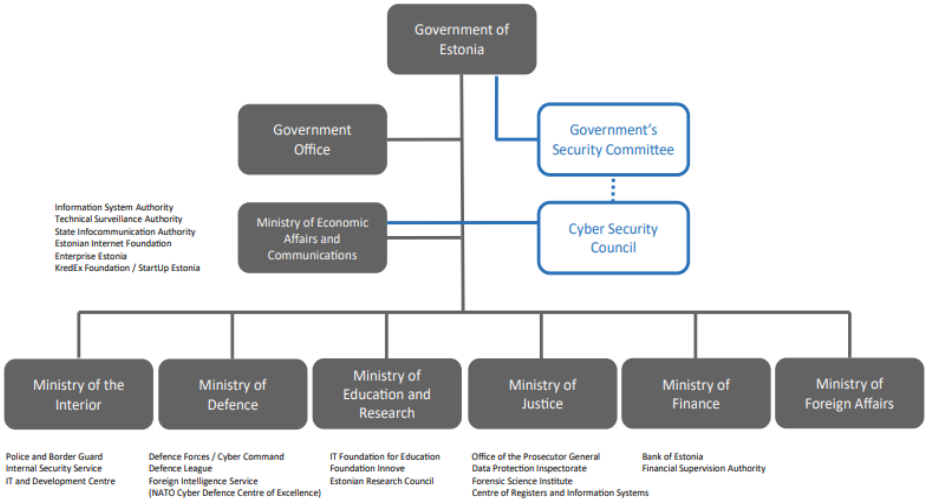


Figure 3: System for management of the cybersecurity sector

Source: Estonian Cyber Security Strategy.

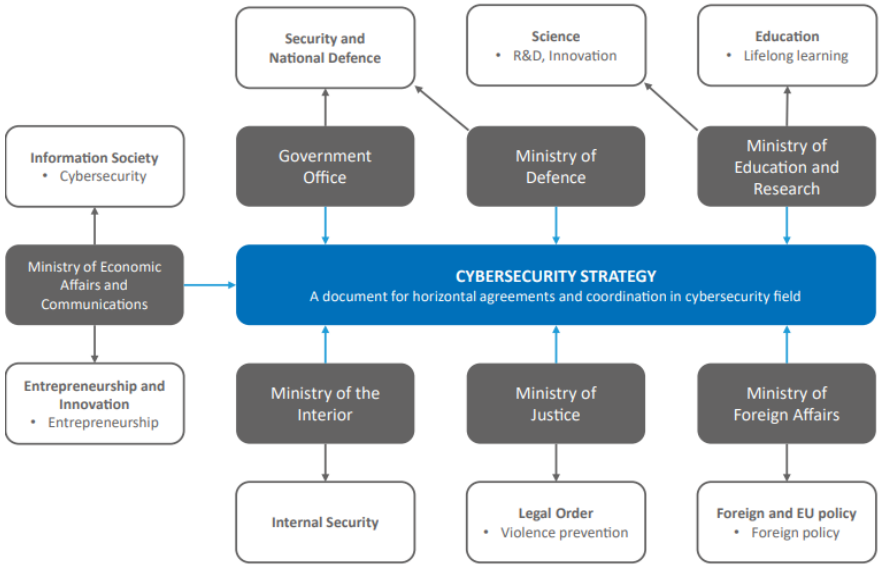
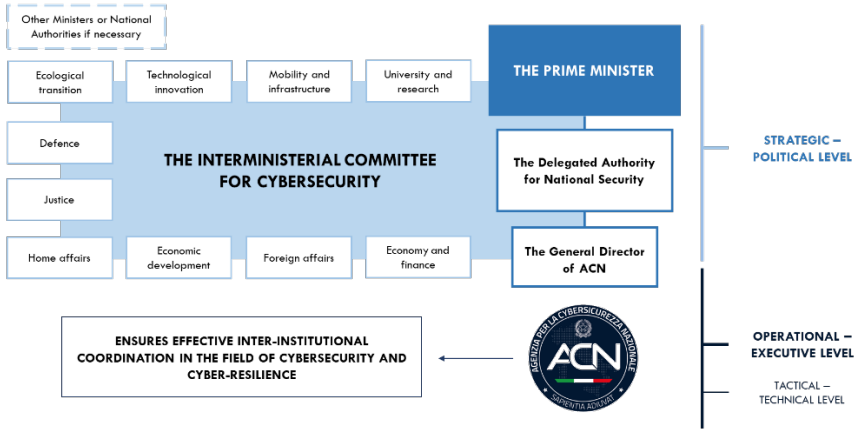


Figure 2: Performance areas connected to planning activities necessary for implementing the objectives of the Cybersecurity Strategy

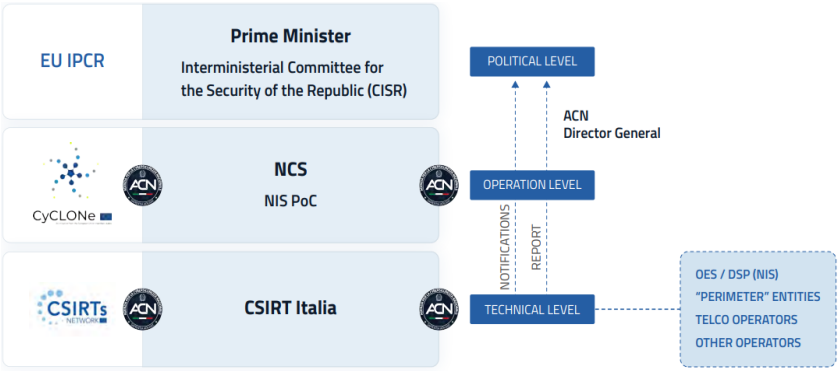
Source: Estonian Cyber Security Strategy.

A.7 ITALY



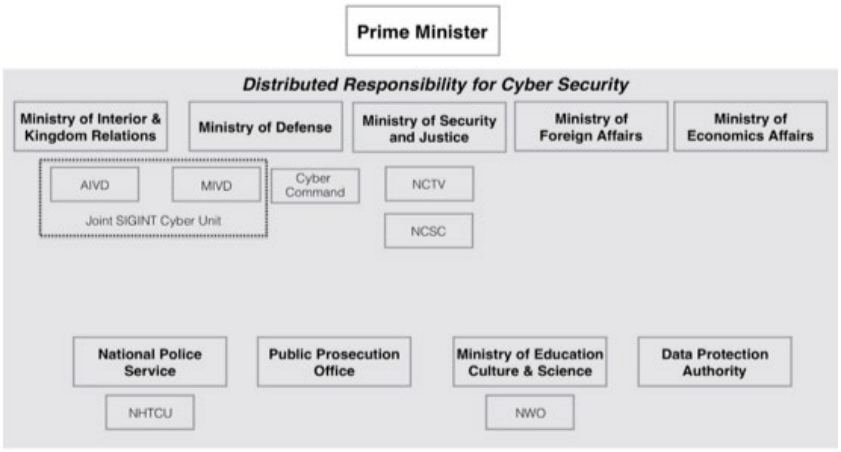
Source: Italian Cyber Security Strategy.

Source: Italian Cyber Security Strategy.



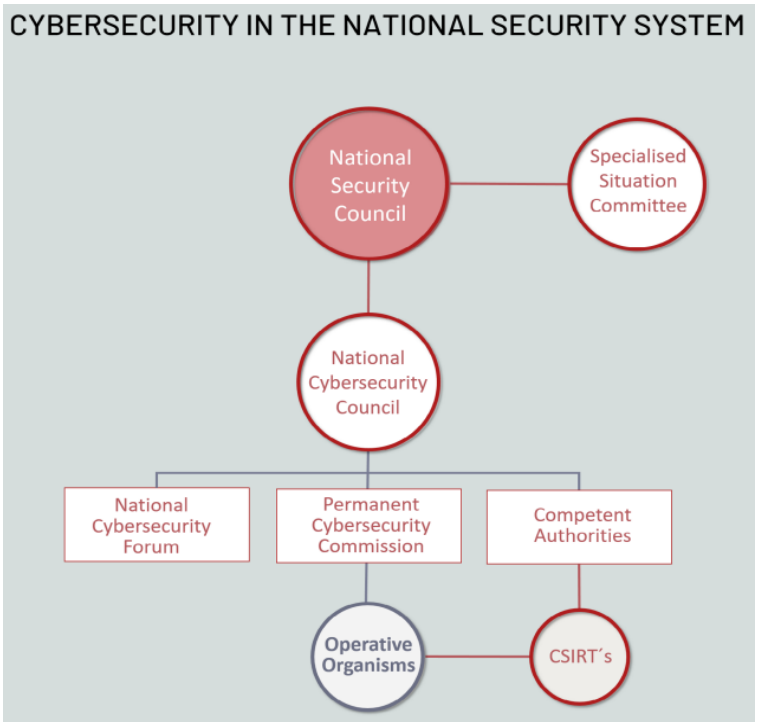
Source: Italian Cyber Security Strategy.

A.8 NETHERLANDS



Source: The Netherlands cyber readiness glance paper.

A.9 SPAIN



Source: National Cybersecurity Strategy 2019.

B ANNEX: EXISTING SETS OF KPIS

B.1 NCAF INDICATORS

This section presents the ENISA National Capabilities Assessment Framework indicators. The indicators are organised by cluster. For each cluster, a table presents the comprehensive set of indicators in the form of questions representative of a given maturity level.

B.1.1 Cluster #1: Cybersecurity governance and standards

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
1 – Develop national cyber contingency plans	a	Do you cover the objective in your current NCSS or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Did you start to work on building national cyber contingency plans? *e.g.,* laying out the general goals, scope and/or principles of the contingency plans…	Do you have a doctrine/national strategy that includes cybersecurity as a crisis factor (i.e., a blueprint, a policy, etc.)?	Do you have a national-level cyber crisis management plan?	Are you satisfied with the number or percentage of critical sectors included in the national cyber contingency plan?	Do you have a lesson learning process in place following cyber exercises or actual crises at national level?
	2	Is it generally understood that cyber incidents constitute a crisis factor that could threaten national security?	Do you have a hub to acquire information and inform decision makers? *i.e.,* any methods, platforms or locations to ensure all crisis response actors can access the same, real-time information about the cyber-crisis.	Do you have national-level cyber crisis-specific procedures?	Do you organise activities (i.e., exercises) related to national cyber contingency planning frequently enough?	Do you have a process to test the national plan regularly?
	3	Have studies (technical, operational, political) been performed on the field of cyber contingency planning?	Are the relevant resources engaged to oversee the development and execution of national cyber contingency plans?	Do you have a communications team specially trained to respond to cyber crises and inform the public?	Do you have sufficient people dedicated to crisis planning, look at the lessons learnt and implement change?	Do you have adequate tools and platforms to build situational awareness?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	4	-	Do you have a cyber threat assessment methodology at national level that includes procedures for impact assessment?	Do you engage all relevant national stakeholders (national security, defence, civil protection, law enforcement, ministries, authorities, etc.?)	Do you have sufficient people trained to respond to cyber crises at national level?	Do you follow a specific maturity model to monitor and improve the cyber contingency plan?
	5	-	-	Do you have adequate crisis management facilities and situation rooms?	-	Do you have resources either specialised in threat anticipation or working on prospective cybersecurity to address future crisis or tomorrow's challenges?
	6	-	-	Do you engage with international stakeholders in the EU if required?	-	-
	7	-	-	Do you engage with international stakeholders in non-EU countries if required?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
2 – Establish baseline security measures	a	Do you cover the objective in your current NCSS or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Have you performed a study to identify requirements and gaps for public organisations based on internationally recognised standards? *e.g.,* ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	Are the security measures drawn in compliance with international/national standards?	Are baseline security measures mandatory?	Is there a process to frequently update baseline security measures?	Do you have a process to harden ICT when incidents fail to be addressed by the measures?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	2	Have you performed a study to identify requirements and gaps for **private** organisations based on internationally recognised standards? e.g., ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS...	Are private sector and other stakeholders consulted when defining baseline security measures?	Do you implement horizontal security measures across critical sectors?	Is there a monitoring mechanism in place to examine uptake of baseline security measures?	Do you evaluate the relevance of new standards that are developed in response to the latest development in the threat landscape?
	3	-	-	Do you implement sector specific security measures across critical sectors?	Is there a national authority for checking whether baseline security measures are enforced or not?	Do you have or promote a national coordinated vulnerability disclosure (CVD) process?
	4	-		Are baseline security measures in line with relevant certification schemes?	Do you have a process in place to identify non-compliant organisations within a specific period of time?	-
	5	-	-	Is there a self-risk assessment process in place for baseline security measures?	Is there an auditing process to ensure that the security measures are applied properly?	-
NCSS objective	**#**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
2 – Establish baseline security measures	6	-	-	Do you review mandatory baseline security measures in the procurement process of governmental bodies?	Do you define or actively encourage the adoption of secure standards for the development of critical IT/OT products (medical equipment, connected and autonomous vehicles, professional radio, heavy industry equipment…)?	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
3 – Secure digital identity and build trust in digital public services	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Have you performed studies or gap analyses to identify the needs to secure digital public services to citizens and businesses?	Do you perform risk analyses to determine the risk profile of the assets or services before moving them to the cloud or to engage any digital transformation projects?	Do you promote privacy-by-design methodologies in all e-Government projects?	Do you collect indicators on cybersecurity incidents involving the breach of digital public services?	Do you participate in European working groups to maintain standards and/or design new requirements for electronic trust services (e-signatures, e-seals, e-registered delivery services, time stamping, website authentication)? *e.g.,* ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU...
	2	-	Do you have a strategy to build or promote secure national electronic identification schemes (eIDs) for citizens and businesses?	Do you include private stakeholders in designing and delivering secure digital public services?	Have you implemented mutual recognition of e-identification means with other Member States?	Do you actively participate in peer reviews as part of eID schemes notification to the European Commission?
	3	-	Do you have a strategy to build or promote secure national electronic trust services (e-signatures, e-seals, e-registered delivery services, time stamping, website authentication) for citizens and businesses?	Do you implement a minimum security baseline for all digital public services?	-	-
NCSS objective	**#**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
3 – Secure digital identity and build trust in digital public services	4	-	Do you have a strategy on Governmental cloud (a cloud computing strategy targeted towards the government and public bodies such as ministries, governmental agencies and public administrations…) that takes into account the implications for security?	Are any electronic identification schemes available to citizens and businesses with a substantial or high assurance level as defined in the Annex of the eIDAS Regulation (EU) No 910/2014?	-	-
	5	-	-	Do you have digital public services requiring electronic identification schemes with a substantial or high assurance level as defined in the Annex of the eIDAS Regulation (EU) No 910/2014?	-	-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	6	-	-	Do you have trust services providers for citizens and businesses (e-signatures, e-seals, e-registered delivery services, time stamping, website authentication)?	-	-
	7	-	-	Do you foster the adoption of baseline security measures for all cloud deployment models (e.g., Private, Public, Hybrid. IaaS, PaaS, SaaS)?	-	-

Source: ENISA (2020), National capabilities assessment framework.

B.1.2 Cluster #2: Capacity-building and awareness

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
4 – Establish an incident response capability	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Do you have informal incident response capabilities managed within or between public and private sectors?	Do you have at least one official national CSIRT ?	Do you have incident response capabilities for the sectors referred to in annex II of the NIS Directive?	Have you defined and promoted standardised practices for incident response procedures and incident classification schemes?	Do you have any mechanisms for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities?
	2	-	Does your national CSIRT(s) have a clearly defined scope of intervention? *e.g.,* depending on the targeted sector, the types of incidents, the impacts	Is there a CSIRT cooperation mechanism in your country to respond to incidents?	Do you evaluate your incident response capability to ensure that you have the adequate resources and skills to carry out the tasks set out in point (2) of Annex I of the NIS Directive?	-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	3	-	Does your national CSIRT(s) have clearly defined relationships with other national stakeholders concerning national cybersecurity landscape and incident response practice (e.g., LEA, military, ISPs, NCSC)?	Does your national CSIRT(s) have an incident response capability in accordance with Annex I of the NIS Directive? *i.e.,* availability, physical security, business continuity, international cooperation, incident monitoring, early warning and alerts capacity, incident response, risk analysis and situational awareness, cooperation with private sector, standard practices...	-	-
	4	-		Is there a cooperation mechanism with other neighbouring countries regarding incidents?	-	-
	5	-	-	Have you formally defined clear incident handling policies and procedures?	-	-
NCSS objective	**#**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
4 – Establish an incident response capability	6	-	-	Is your national CSIRT(s) participating in cybersecurity exercises both at national and international level?	-	-
	7	-	-	Is your national CSIRT(s) affiliated with FIRST (Forum of Incident Response and Security Teams)?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
5 – Raise user awareness	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
5 – Raise user awareness	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Is there a minimal recognition from the government, private sector or general users, that there is a need to raise awareness on cybersecurity and privacy issues?	Have you identified a specific target audience for user awareness? *e.g.,* general users, young people, business users (which can be broken down further: SMEs, OES, DSPs etc)	Have you developed communication plans/strategy for the campaigns?	Do you draw up metrics for evaluating your campaign during the planning stage?	Do you have mechanisms in place to ensure that awareness campaigns are constantly relevant regarding technological advancement, changes to the threat landscape, legal regulations and national security directives?
	2	Are public agencies conducting cybersecurity awareness campaigns within their organisation on an ad-hoc basis? e.g., in the wake of a cybersecurity incident.	Do you draw up a project plan to raise awareness on information security and privacy issues?	Do you have a process for creating content at governmental level?	Do you evaluate your campaigns after execution?	Do you perform periodic evaluation or study to measure attitude shift or behaviour changes regarding cybersecurity and privacy matters across private and public sectors?
	3	Are public agencies conducting cybersecurity awareness campaigns to the general public on an ad-hoc basis? *E.g.,* in the wake of a cybersecurity incident.	Do you have resources available and easily identifiable (*e.g.,* a single online portal, awareness kits) for any users who seek to educate themselves on information on cybersecurity and privacy issues?	Do you have any mechanisms to identify target areas for raising awareness (i.e., ENISA Threat landscape, national landscapes, international landscapes, feedback from national cybercrime centres, etc.) ?	Do you have any mechanisms in place to identify the most relevant media or communication channel depending on the target audience to maximise outreach and engagement? *e.g.,* different types of digital media, brochures, emails, teaching material, posters in busy areas, TV, radio…	Do you consult with behavioural experts to tailor your campaign towards the target audience?
	4	-	-	Do you bring stakeholders with experts and communications teams together to create content?		-
	5	-	-	Do you involve and engage the private sector in your awareness efforts to promote and disseminate the messages to a wider audience?	-	-
	6	-	-	Do you prepare specific awareness initiatives for executives in the public, private, academic or civil society sectors?	-	-
	7	-	-	Do you participate in ENISA European Cybersecurity Month (ECSM) campaigns?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
6 – Organise cybersecurity exercises	a	Do you cover the objective in your current NCSS or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
6 – Organise cybersecurity exercises	1	Do you conduct crisis exercises in other sectors (other than cybersecurity) at a national level or pan-European level?	Do you have a cybersecurity exercise program at national level?	Do you involve all related authorities of public administration? (Even if the scenario is sector-specific)	Do you write after action reports/evaluation reports?	Do you have a lesson learnt analysis capacity for cyber (reporting processes, analysis, mitigation)?
	2	Do you have resources allocated to crisis management exercise design and planning?	Do you carry out or prioritise cyber crisis management exercises on vital societal functions and critical infrastructure?	Do you involve the private sector in the planning and execution of the exercises?	Do you test national-level plans and procedures?	Do you have an established lessons learnt process?
	3	-	Have you identified a coordinating body to oversee the design and planning of cybersecurity exercises (public agency, consultancy...)?	Do you organise sector specific exercises at national and/or international level?	Do you participate in cybersecurity exercises at pan-European level?	Do you adapt the exercise scenarios depending on the latest developments (technological advancements, global conflicts, threat landscape…)?
	4	-	-	Do you organise exercises across all critical sectors mentioned in Annex II of the NIS Directive?	-	Do you align your crisis management procedures with other Member States to ensure effective pan-European crisis management?
	5	-	-	Do you organise inter-sectorial and/or cross-sectorial cybersecurity exercises?	-	Do you have a mechanism in place to quickly adapt the strategy, plans and procedures from the lessons learnt during the exercises?
	6	-	-	Do you organise cybersecurity exercises specific to various levels? (Technical and operational level, procedure level, decision-making level, political level…)	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
7 – Strengthen training and educational programmes	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Do you consider developing cybersecurity training and educational programmes?	Do you establish courses dedicated to cybersecurity?	Does your country encompass cybersecurity culture at the early stage of students' education path? For example, do you favour cybersecurity in middle-school and high-school?	Do you urge personnel in the private and public sector to be accredited or certified?	Do you have mechanisms in place to ensure that trainings and educational programmes are constantly relevant regarding current and emerging technological developments, changes to the threat landscape, legal regulations and national security directives?
	2	-	Do universities of your country offer PhDs in cybersecurity as an independent discipline and not as a computer science subject?	Do you have national research labs and educational institutions which are specialized in cybersecurity?	Has your country developed cybersecurity training or mentorship programs to support national start-ups and SMEs?	Do you establish academic centres of excellence in cybersecurity to act as hubs of research and education?
	3	-	Do you plan to train educators, independently of their field, on information security and privacy issues? *e.g.,* online safety, personal data protection, cyber-bullying.	Do you encourage/fund dedicated cybersecurity courses and training plans for employee's member-state employment agencies?	Do you actively promote the addition of information security courses in higher education not only for computer science students but also to any other professional speciality? *e.g.,* courses tailored to the needs of that profession.	Are academic institutions participating in leading discussions in the area of cybersecurity education and research internationally?
	4	-	-	Do you have cybersecurity courses and/or specialised curriculum for EQF (European Qualifications Framework) level 5 to 8?	Do you assess the skill gap (cybersecurity workers shortage) in the area of information security on a regular basis?	-
	5	-	-	Do you encourage and/or support initiatives to include internet safety courses in primary and secondary level education?	Do you foster networking and information sharing between academic institutions, at both national and international level?	

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
7 - Strengthen training and educational programmes	6	-	-	Do you fund or offer for free basic cybersecurity trainings to citizens?	Do you involve the private sector in any form in cybersecurity education initiatives? *e.g.,* course design and delivery, internships, work placements…	-
	7	-	-	Do you organise annual information security events (e.g., hacking contests or hackathons)?	Do you implement funding mechanisms to encourage the uptake of cybersecurity degrees? *e.g.,* scholarships, guaranteed apprenticeship/internship, guaranteed jobs in specific industry or roles in public sector	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
8 – Foster R&D	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Have you performed studies or analyses to identify cybersecurity R&D priorities?	Do you have a process to define R&D priorities (e.g., emerging topics for deterring, protecting, detecting, and adapting to new kinds of cyber-attacks)?	Is there a plan to link R&D initiatives with real economy?	Are R&D cybersecurity initiatives in line with relevant strategic objectives, e.g., DSM, H2020, Digital Europe, EU cybersecurity strategy?	Do you pursue at a national level cooperation with any international R&D initiatives related to cybersecurity?
	2	-	Is the private sector involved in setting up R&D priorities?	Are there any national projects related to cybersecurity in place?	Is there an evaluation scheme in place for R&D initiatives?	Are R&D priorities aligned with current or upcoming regulation (national level)?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
8 – Foster R&D	3	-	Is academia involved in setting up R&D priorities?	Do you have local/regional start-up ecosystems and other networking channels (e.g., technological parks, innovation clusters, networking events/platforms) to foster innovation (including for cybersecurity start-ups)?	Are there any cooperation agreements with universities and other research facilities?	Do you participate in leading discussions in one or many cutting-edge R&D topics at international level?
	4	-	Are there any national R&D initiatives related to cybersecurity?	Is there investment in cybersecurity R&D programs in academia and the private sector?	Is there a recognized institutional body overseeing cybersecurity R&D activities?	-
	5	-	-	Do you have industrial research chairs in universities to bridge research subjects and market needs?	-	-
	6	-	-	Do you have dedicated R&D funding programmes for cybersecurity?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
9 – Provide incentives for the private sector to invest in security measures	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Is there an industrial policy or political will to encourage the development of the cybersecurity industry?	Is the private sector involved in the design of incentives?	Are there economic/regulatory or other types of incentives in place to promote cybersecurity investments?	Are there any private actors that react to incentives by investing in security measures? *e.g.,* investors specialised in cybersecurity and non-specialised investors	Do you focus incentives on cybersecurity topics depending on the latest threat developments?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
9 – Provide incentives for the private sector to invest in security measures	2	-	Have you identified specific cybersecurity topics to be developed? *e.g.,* cryptography, privacy, new form of authentication, AI for cybersecurity…	Do you provide support (e.g., tax incentives) for cybersecurity start-ups and SMEs?	Do you provide incentives for the private sector to focus on the security of cutting-edge technologies? *e.g.,* 5G, artificial intelligence, IoT, quantum computing…	-
	3	-	-	Do you provide tax incentives or other financial motivation for private sector investors in cybersecurity start-ups?	-	-
	4	-	-	Do you facilitate access for cybersecurity start-ups and SMEs in the public procurement process?	-	-
	5	-	-	Is there budget available to provide incentives for the private sector?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
10 – Improve the cybersecurity of the supply chain	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Have you performed a study on security good practices for supply chain management used by procurement in various industry segments and/or in public sector?	Do you perform cybersecurity assessments all along the supply chain of ICT services and products in critical sectors (as identified in Annex II of the NIS (2016/1148) Directive)?	Do you use a security certification scheme for ICT-based products and services? *e.g.,* SOG-IS MRA in Europe (Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement), Common Criteria Recognition Arrangement (CCRA), national initiatives, sectorial initiatives…	Do you have a process in place to update the cybersecurity assessments of the supply chain of ICT services and products in critical sectors (as identified in Annex II of the NIS (2016/1148) Directive)?	Do you have detection probes in key elements in the supply chain to detect early sign of compromise? *e.g.,* security controls at ISP-level, security probes in major infrastructure components…-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
10 – Improve the cybersecurity of the supply chain	2	-	Do you apply standards in public administrations' procurement policies to ensure that providers of ICT products or services meet baseline information security requirements? *e.g.,* ISO/IEC 27001 and 27002, ISO/IEC 27036…	Do you actively promote security and privacy by design best practices in ICT products and services development? *e.g.,* secure software development lifecycle, IoT lifecycle	Do you have a process in place to identify cybersecurity weak links in the supply chain of critical sectors (as identified in Annex II of the NIS (2016/1148) Directive)?	-
	3	-	-	Do you develop and provide a centralised catalogues with extended information of existing information security and privacy standards that are scalable for, and applicable by, SMEs?	Do you have mechanisms in place to ensure that ICT products and services that are critical to OES are cyber-resilient (*i.e.,* the ability to maintain availability and safety against a cyber incident)? *e.g.,* through testing, regular assessments, detection of compromised elements…	-
	4	-		Do you actively participate in the design of an EU certification framework for ICT digital products, services and processes as established in the EU cybersecurity act (Regulation (EU) 2019/881)? *e.g.,* participation in the European Cybersecurity Certification Group (ECCG), promoting technical standards and procedures for ICT products/services security	Do you promote the development of certification schemes targeted at SMEs to boost information security and privacy standard adoption?	-
	5	-	-	Do you provide any types of incentives to SMEs to adopt security and privacy standards?	Do you have any provisions in place to encourage large companies to increase the cybersecurity of small enterprises in their supply chains? *e.g.,* cybersecurity hub, training and awareness campaigns…	-
	6	-	-	Do you encourage software vendors to support SMEs by ensuring secure default configurations in products targeting small organizations?	-	-

Source: ENISA (2020), National capabilities assessment framework.

B.1.3 Cluster #3: Legal and regulatory

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
11 – Protect critical information infrastructure, OES, and DSP	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Is there a general understanding that CII operators contribute to national security?	Do you have a methodology to identify essential services ?	Have you implemented the NIS (2016/1148) Directive?	Do you have a procedure to update the risk registry?	Do you create and update threat landscape reports?
	2	-	Do you have a methodology for the identification of CIIs?	Have you implemented the ECI (2008/114) Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection?	Do you have other mechanisms in place to measure that the technical and organisational measures implemented by OES are appropriate to manage the risks posed to the security of network and information systems? e.g., regular cybersecurity audits, national framework for the implementation of standard measures, technical tools provided by the government such as detection probes or system-specific configuration review...	Depending on the latest developments in the threat landscape, are you able to onboard a new sector in your CIIP action plan?
	3	-	Do you have a methodology to identify OES?	Do you have a national registry for identified OES per critical sector?	Do you review and consequently update the list of identified OES at least every two years?	Depending on the latest developments in the threat landscape, are you able to adapt new requirements in your CIIP action plan?

NCSS objective	#					
11 – Protect critical information infrastructure, OES, and DSP	4	-	Do you have a methodology to identify digital service providers?	Do you have a national registry for identified digital service providers?	Do you have other mechanisms in place to measure that the technical and organisational measures implemented by digital service providers are appropriate to manage the risks posed to the security of network and information systems? e.g., regular cybersecurity audits, national framework for the implementation of standard measures, technical tools provided by the government such as detection probes or system-specific configuration review...	-
	5	-	Do you have one or more national authority providing oversight on critical information infrastructure protection and the security of network and information systems? e.g., as required per the NIS (2016/1148) Directive	Do you have a national risk registry for identified or known risks?	Do you review and consequently update the list of identified digital service providers at least every two years?	-
	6	-	Do you develop sector-specific protection plans? e.g., including baseline cybersecurity measures (mandatory or guidelines)	Do you have a methodology to map CII dependencies?	Do you use a security certification scheme (national or international) to help OES and digital service providers identify secure ICT products? e.g., SOG-IS MRA in Europe, national initiatives…	-
	7	-	-	Do you deploy risk management practices to identify, quantify and manage risks related to CIIs at a national level?	Do you use a security certification scheme or qualification procedure to assess service providers working with OES? e.g., service providers in the field of incident detection, incident response, cybersecurity audit, cloud services, smart cards…	-
	8	-	-	Do you engage in a consultation process to identify cross border dependencies?	Do you have mechanisms in place to measure the compliance level of OES and digital service providers with regards to baseline cybersecurity measures?	-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
11 – Protect critical information infrastructure, OES, and DSP	9			Do you have a single point of contact responsible for coordinating issues related to the security of network and information systems at national level and cross-border cooperation at Union level?	Do you have any dispositions in place to ensure the continuity of the services provided by critical information infrastructures? e.g., crisis anticipation, procedures to rebuild critical information systems, business continuity without IT, air gap backup procedures…	
	10			Do you define baseline cybersecurity measures (mandatory or guidelines) for digital service providers and all sectors identified in Annex II of the NIS (2016/1148) Directive?		
	11	-	-	Do you provide tools or methodologies to detect cyber incidents?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
12 – Address cybercrime	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Have you performed a study to identify the law enforcement requirements (legal basis, resources, skills…) to effectively address cybercrime?	Is your national legal framework fully complying with the relevant EU legal framework, including the Directive 2013/40/EU on attacks against information systems? e.g., Illegal access to information systems, Illegal system interference, Illegal data interference, Illegal interception, Tools used for committing offences...	Do you have units dedicated to handle cybercrime in prosecution offices?	Do you collect statistics following the provisions of article 14 (1) of Directive 2013/40/EU (Directive on attacks against information systems) ?	Do you have interinstitutional training or training workshops for LEAs, Judges, prosecutors and national/governmental CSIRTs at a national level and/or at a multilateral level?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	2	Have you performed a study to identify the prosecutors and judges' requirements (legal basis, resources, skills…) to effectively address cybercrime?	Do you have any legal provision addressing online identity theft and personal data theft?	Do you have a dedicated budget allocated to cybercrime units?	Do you collect separate statistics on cybercrime? e.g., operational statistics, statistics on cybercrime trends, statistics on cybercrime proceeds and induced damage…	Do you participate in coordinated actions at international level to disrupt criminal activities? e.g. infiltration of criminal hacking forums, organised cybercrime groups, dark web markets and botnets takedowns…
	3	Has your country signed the Council of Europe Budapest Convention on Cybercrime?	Do you have any legal provision addressing online intellectual property and copyright infringements?	Have you established a central body/entity to coordinate the activities in the area of fighting cybercrime?	Do you evaluate the adequacy of the training provided to LEAs, judiciary and national CSIRT(s) personnel to address cybercrime?	Is there clear segregation of duties across CSIRTs, LEAs and the judiciary (prosecutors and judges) when they cooperate for addressing cybercrimes?
	4		Do you have any legal provision addressing online harassment or cyber-bullying?	Have you established cooperation mechanisms between relevant national institutions involved in fighting cybercrime, including law enforcement national CSIRTs?	Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to cybercrime units within LEAs?	Does your regulatory framework facilitate the cooperation between CSIRTs/LE and judiciary (prosecutors and judges)?
NCSS objective	**#**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
12 – Address cybercrime	5		Do you have any legal provision addressing computer-related fraud? e.g., compliance with provisions the Council of Europe Budapest Convention on Cybercrime	Do you cooperate and share information with other Member States in the area of fighting against cybercrime?	Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to cybercrime units within prosecution authorities?	Do you participate in building and maintaining standardised tools and methodologies, forms and procedures to be shared with EU stakeholders (LEAs, CSIRTs, ENISA, Europol's EC3…)?
	6	-	Do you have any legal provision addressing child online protection? e.g., compliance with provisions of Directive 2011/93/EU and the Council of Europe Budapest Convention on Cybercrime...	Do you cooperate and share information with EU Agencies (e.g., Europol's EC3, Eurojust, ENISA) in the area of fighting against cybercrime?	Do you have units dedicated courts or specialized judges to handle cybercrime cases?	Do you have any advanced mechanisms in place to deter individuals from being attracted to, or becoming involved in, cybercrime?
	7	-	Have you identified an operational national point of contact to exchange information and to answer urgent information requests from other Member States relating to offences set out in Directive 2013/40/EU (Directive on attacks against information systems)?	Do you have the adequate tools to address cybercrime? e.g., cybercrime taxonomy and classification, tools to collect electronic evidence, computer forensics tools, trusted sharing platforms...	Do you have any dispositions dedicated to providing support and assistance to victims of cybercrimes (general users, SMEs, large companies)?	Does your country use EU Blueprint and/or the Law Enforcement Emergency Response Protocol (EU LE ERP) to effectively respond to large scale cyber incidents?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	8		Does your law enforcement agency include a dedicated cybercrime unit?	Do you have standard operating procedures to handle e-evidence?	Have you established an inter-institutional framework and cooperation mechanisms between all relevant stakeholders (e.g., LEA, national CSIRT, judiciary communities), including private sector (e.g., operators of essential services, service providers) where appropriate, to respond to cyber-attacks?	-
	9		Have you designated, in accordance with Art. 35. Budapest Convention, a 24/7 point of contact?	Does your country participate in training opportunities offered and/or supported by EU Agencies (e.g., Europol, Eurojust, OLAF, Cupola, ENISA)?	Does your regulatory framework facilitate the cooperation between CSIRTs and LE?	-
NCSS objective	**#**	**Level 1**	**Level 2**	**Level 3**	**Level 4**	**Level 5**
12 – Address cybercrime	10	-	Have you designated an operational 24/7 national point of contact for the EU Law Enforcement Emergency Response Protocol (EU LE ERP) to respond to major cyber-attacks?	Is your country considering adopting the 2nd additional protocol to the Council of Europe Budapest Convention on Cybercrime?	Do you have mechanisms in place (e.g., tools, procedures) to facilitate the information exchange and the cooperation between CSIRT/LE and possibly judiciary (prosecutors and judges) in the area of fighting against cybercrime?	-
	11		Do you provide specialised training to stakeholders involved in addressing cybercrime (LEAs, judiciary, CSIRTs) on a regular basis? e.g., training sessions on filing/prosecuting cyber-enabled crimes, trainings on collecting electronic evidence and ensuring integrity throughout the digital chain of custody and computer forensics, among others			
	12		Has your country ratified/acceded the Council of Europe Budapest Convention on Cybercrime?		-	-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
	13	-	Has your country signed and ratified the Additional Protocol (criminalisation of acts of a racist and xenophobic nature committed through computer systems) to the Council of Europe Budapest Convention on Cybercrime?	-	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
13 – Establish incident reporting mechanisms	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Do you have informal information sharing mechanisms on cybersecurity incidents between private organisations and national authorities?	Do you have an incident reporting scheme for all the sectors under the annex II of the NIS Directive?	Do you have a mandatory incident reporting scheme that is functioning in practice?	Do you have a harmonised procedure for sectorial incident reporting schemes?	Do you create annual incidents report?
	2	-	Have you implemented the notification requirements for telecommunication service providers in compliance with article 40 of the Directive (EU 2018/1972)? The Directive requires that Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.	Is there a coordination/cooperation mechanism for incident reporting obligations regarding GDPR, NISD, article 40 (ex-art13a) and eIDAS?	Do you have an incident reporting scheme for sectors others than the ones under the NIS Directive?	Are there any cybersecurity landscape reports in place or other kinds of analysis prepared by the entity that receives the incident reports?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
13 – Establish incident reporting mechanisms	3	-	Have you implemented the notification requirements for trust services providers in compliance with article (19) of the eIDAS Regulation (Regulation (EU) No 910/2014)? The article (19) requires, among other requirements, that providers of trust services notify the supervisory body about significant incidents/breaches.	Do you have the adequate tools to ensure the confidentiality and integrity of information shared via the various reporting channels?	Do you measure the effectiveness of incident reporting procedures? *e.g.,* indicators on incidents that have been reported through the appropriate channels, timing of the incident report…	-
	4	-	Have you implemented the notification requirements for digital service providers in compliance with article (16) of the NIS Directive? The article (16) requires that digital service providers notify the competent authority or national CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union.	Do you have a platform/tool to facilitate the reporting process?	Do you have a common taxonomy at national level for incident classification and root cause categories?	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
14 – Reinforce privacy and data protection	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Have you performed studies or analyses to identify areas of improvement to better protect the rights of citizen's privacy?	Is the national data protection authority involved in cybersecurity related issue areas (e.g., drafting new cybersecurity laws and regulations, defined minimum security measures)?	Do you promote best practices on security measures and data protection by design for the public and/or private sector?	Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to the data protection authority?	Do you have any mechanisms in place to monitor the latest technological developments in order to adapt relevant guidelines and legal provisions/obligations?
	2	Have you developed a legal basis at the national level to enforce the General Data Protection Regulation (Regulation EU No 2016/679)? e.g., maintain or introduce more specific provisions or limitations to the rules of the Regulation	-	Do you launch awareness raising and training programs around this topic?	Do you encourage organisations and businesses to get certified against ISO/IEC 27701:2019 on Privacy Information Management System (PIMS)?	Do you actively participate/promote R&D initiatives regarding privacy enhancing technologies (PET)?
	3	-	-	Do you coordinate incident reporting procedures with the DPA?	-	-
	4	-	-	Do you promote and support development of technical standards on information security and privacy? Are they specifically tailored to small and medium enterprises (SMEs)?	-	-
	5	-	-	Do you provide practical and scalable guidelines to support different types of data controllers on meeting the privacy and data protection legal requirements and obligations?	-	-

Source: ENISA (2020), National capabilities assessment framework.

B.1.4 Cluster #4: Cooperation

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
15 – Establish a public-private partnership (PPPs)	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Is it generally understood that PPPs contribute to the raising of the level of cybersecurity in the country by different means? *e.g.,* sharing interests in the growth of the cybersecurity industry, cooperation in building a relevant cybersecurity regulatory framework, foster R&D...	Do you have a national action plan for establishing PPPs?	Have you established national public-private partnerships?	Have you established cross-sector PPPs?	Depending on the latest technological and regulatory developments, are you able to adapt or create PPPs?
	2	-	Do you establish a legal or contractual basis (specific laws, NDAs, intellectual property) to scope PPPs?	Have you established sector-specific PPPs?	In the established PPPs, do you also focus on public-public and private-private cooperation?	
	3	-	-	Do you provide funding for the establishment of PPPs?	Do you promote PPPs among small and medium enterprises (SMEs)?	-
	4	-	-	Do public institutions lead the PPPs overall? *i.e.,* one single point of contact from the public sector governing and coordinating the PPP, public bodies agree in advance on what they want to achieve, clear guidelines from public administrations on their needs and limitations to the private sector…	Do you measure the outcomes of PPPs?	-
	5	-	-	Are you a member of the European Cyber Security Organisation (ECSO) contractual public-private partnership (cPPP)?	-	-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
15 – Establish a public-private partnership (PPPs)	6	-	-	Do you have one or several PPPs working on CSIRT activities?	-	-
	7			Do you have one or several PPPs working on critical information infrastructure protection issues?		
	8	-	-	Do you have one or several PPPs working on raising cybersecurity awareness and skills development?	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
16 – Institutionalise cooperation between public agencies	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Do you have informal cooperation channels between public agencies?	Do you have a national cooperation scheme focused on cybersecurity? *e.g.,* advisory boards, steering groups, forums, councils, cyber centres or expert meeting groups	Do public authorities participate in the cooperation scheme?	Do you ensure cooperation channels dedicated to cybersecurity exist at least between the following public bodies: intelligence services, domestic law enforcement, prosecution authorities, government actors, national CSIRT and the military?	Are public agencies provided with uniform minimum information on the latest developments of the threat landscape and cybersecurity situational awareness?
	2	-	-	Have you established cooperation platforms to exchange information?	Do you measure the successes and limits of the different cooperation scheme in fostering effective cooperation?	-

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
16 – Institutionalise cooperation between public agencies	3	-	-	Have you defined the scope of cooperation platforms (e.g., tasks and responsibilities, number of issue areas)?	-	-
	4	-	-	Do you organise annual meetings?	-	-
	5	-	-	Do you have cooperation mechanisms between competent authorities across geographical regions? *e.g.,* network of security correspondents per region, cybersecurity officer in regional economic chambers…	-	-

Source: ENISA (2020), National capabilities assessment framework.

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
17 – Engage in international cooperation (not only with EU MS)	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	Do you have an action plan that is formally defined and documented?	Do you review your action plan regarding the objective to test its performance?	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
	b		Did you define intended results, guiding principles or key activities of your action plan?	Do you have an action plan with a clear resource allocation and governance?	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	
	c		If relevant, is your action plan implemented and already effective on a limited scope?			
	1	Do you have an international engagement strategy?	Do you have cooperation agreements with other countries (bilateral, multilateral) or partners in other countries? *e.g.,* information sharing, capacity-building, assistance…	Do you exchange information at strategic level? *e.g.,* high-level policy, risk perception...	Are national cybersecurity public agencies in your country involved in international cooperation schemes?	Do you lead discussions on one or many topics within multilateral agreements?
	2	Do you have informal cooperation channels with other countries?	Do you have a single point of contact that can exercise a liaison function to ensure cross-border cooperation with Member State authorities (cooperation group, CSIRTs network…)?	Do you exchange information at tactical level? *e.g.,* threat actors bulletin, ISACs, TTPs…	Do you assess, on a regular basis, the outcomes of international cooperation initiatives?	Do you lead discussions on one or many topics within international treaties or conventions?

NCSS objective	#	Level 1	Level 2	Level 3	Level 4	Level 5
17 – Engage in international cooperation (not only with EU MS)	3	Has public leadership expressed intention to engage in international cooperation in the field of cybersecurity?	Do you have dedicated people involved in international cooperation?	Do you exchange information at operational level? *e.g.,* operational coordination information, ongoing incidents, IOCs…	-	Do you lead discussions or negotiations in one or many topics within international groups of experts? *e.g.* The Global Commission on the Stability of Cyberspace (GCSC), ENISA NIS cooperation group, UN Group of Governmental Experts on Information Security (GGE)...
	4	-	-	Do you engage in international cybersecurity exercises?	-	-
	5	-	-	Do you engage in international capacity building initiatives? *e.g.,* trainings, skills development, drafting standard procedures…	-	-
	6	-	-	Have you established mutual assistance agreements with other countries? *e.g.,* LEAs activities, legal proceedings, mutualisation of incident response capabilities, sharing cybersecurity assets…	-	-
	7	-	-	Have you signed or ratified international treaties or conventions in the area of cybersecurity? *e.g.,* International Code of Conduct for Information Security, Convention on Cybercrime	-	-

Source: ENISA (2020), National capabilities assessment framework.

B.2 ITU GLOBAL CYBERSECURITY INDEX KPIS AND SPECIFIC QUESTIONS ON NATIONAL CYBERSECUIRTY STRATEGY

B.2.1 Indicators

1. Legal Measures
    a. Cybercrime substantive law
    b. Cybersecurity regulation/legislation
2. Technical measures
    a. National/Government CIRT, CSIRT, CERT
    b. Sectoral CIRT/CSIRT/CERT
    c. National framework for implementation of cybersecurity standards
    d. Child online protection
3. Organizational measures
    a. National Cybersecurity strategy
    b. Responsible agency
    c. Cybersecurity metrics
4. Capacity development measures
    a. Public cybersecurity awareness campaigns
    b. Training for cybersecurity professionals
    c. Does your government/organization develop or support any educational programmes or academic curricula in cybersecurity
    d. Cybersecurity research and development programmes
    e. National cybersecurity industry
    f. Are there any government incentive mechanisms in place to develop capacity development, a cybersecurity industry?
5. Cooperative measures
    a. Bilateral agreements on cybersecurity cooperation with other countries
    b. Government participation in international mechanisms related to cybersecurity activities
    c. Cybersecurity multilateral agreements
    d. Partnerships with the private sector (PPPs)
    e. Inter-agency partnerships

B.2.2 Questions on national cybersecurity strategy

1. Does your country have a national cybersecurity strategy/policy?
    i. Does it address the protection of national critical information infrastructures, including in the telecommunication sector?
    ii. Does it include reference to the national cybersecurity resilience?
    iii. Does it address the protection of national critical information infrastructures, including in the telecommunication sector?
    iv. Is the national cybersecurity strategy revised and updated on a continuous basis?
    v. Is the cybersecurity strategy open to any form of consultation with national experts in cybersecurity?
2. Is there a defined action plan/roadmap for the implementation of cybersecurity governance?
3. Is there a national strategy for Child Online Protection?

B.3 CYBERSECURITY CAPACITY MATURITY MODEL FOR NATIONS (CMM)

B.3.1 Factor - D 1.1: National Cybersecurity Strategy

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Strategy Development	No national cybersecurity strategy exists, although planning processes for strategy development may have begun.Advice may have been sought from international partners.	Processes for strategy development have been initiated.An outline/draft national cybersecurity strategy has been articulated.Consultation processes have been agreed for key stakeholder groups, including private sector, civil society and international partners.	A national cybersecurity strategy has been published.An assessment of country-specific national cybersecurity risk has been conducted.The strategy reflects the needs and roles of relevant stakeholders across government (national and sub-national), business and civil society.An implementation programme is in place which covers the scope of the strategy.Mechanisms are in place to enable strategy 'owners' to monitor achievement of outcomes, address implementation issues and maintain strategy alignment.	Strategy review and renewal processes are in place.Emerging cybersecurity risks are regularly assessed and used to update the strategy and implementation plan.The impact of the strategy on risk and harm reduction isunderstood and is used to inform funding and priority decisions.	The national cybersecurity strategy and implementation plan are both proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental).The country is an acknowledged authority within the international community and is supportingthe development of national and global cybersecurity strategies.Cybersecurity considerations are embedded within other relevant national-level strategies and implementation programmes.
Content	Various national policies and strategies may exist that refer to cybersecurity, but these are not comprehensive and there is little evidence that these reflect specific national priorities and circumstances.	Content exists that reflects country-specific priorities and circumstances.Links exist between the strategy (or draft strategy) and priorities such as national security,digital strategy and economic development, but these are generally *ad hoc* and lack detail.The strategy (or draft strategy) defines the key outcomes against which success can be evaluated.	The content of the national cybersecurity strategy is based on a comprehensive risk assessment that includes explicit links to wider national level economic and political policies and strategies.The content includes actions to raise public and businessawareness, mitigate cybercrime, establish incident response capability, promote public-private partnership and protect critical infrastructure and the wider economy.Consideration has been given to how the national cybersecurity strategy might incorporate or support wider online policy objectives such as: child protection; the promotion of Human Rights; the promotion of Equality, Diversity and Inclusion; and managing disinformation.	The content takes account of the impact on cybersecurity risk of emerging technologies and their use within critical infrastructure, the wider economy and society.The outcomes defined in the strategy are specific and measurable. Metrics have been defined which enable stakeholders to evaluate theeffectiveness of the strategy in reducing harm.Consideration has been given to how the beneficial outcomes of the strategy can be sustained beyond the strategy's lifetime, including how the maintenance of new capabilities will be financed.	The content takes account of the impact of broader developments on cybersecurity risk (political, economic, social, technical, legal and environmental).The content of the national cybersecurity strategy promotes and encourages bilateral and multilateral co-operation between countries to ensurea secure, resilient and trusted cyberspace.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Implementation and Review	No overarching national cybersecurityimplementation programme has been developed.	A co-ordinated cybersecurity implementation programme is being developed with relevant stakeholders involved, including the private sector and civil society.Actions within the programme have been assigned to specific 'owners' but the availability of adequate resources has not yet been confirmed.Mechanisms to review processes are limited or *ad hoc*.	A detailed implementation plan has been published including actions, responsible entities and resource budgets. The implementation plan involves relevant stakeholders across government and other sectors.A co-ordinating body has been assigned. The body has sufficient authority to ensure that action 'owners' are held to account.The resources required to deliver the actions of the programme have been identified and are in place. Budget shortfalls are identified and escalated to the relevant authority.Programme review processes and metrics are in place that allow progress to be measured and risks, issues and dependencies to be escalated to the relevant authority. These processes are adequately funded.	Outcome-oriented metrics are being used to monitor the impact that the programme is having on risk reduction (and other relevant strategy goals).There is evidence of these metrics being used to refine action plans.Metrics (both progress and outcome-oriented metrics) are drawn from a wide variety of governmental, non-governmental and international sources.There is independent oversight and/or assurance of the programme.	Mechanisms are in place to make more far-reachingchanges to the programme in the event of significant changes in circumstance (political, economic, social, technical, legal and environmental).The programme contributes to the global development of outcome-oriented metrics and their application.
International Engagement	There is limited awareness of the principal international debates relating to cybersecurity policy (suchas cybersecurity norms, mutual legal assistance, Internet Governance, data sovereignty, data protection).The country may benefit from regional/ international operational collaboration networks but does not actively engage.	The country is aware of the existence of international discussions on cybersecurity policy and related issues.The country may, on occasion, participate in regional or international discussions on matters related to cybersecurity issues, but does not generally play an active role.The country may participate in relevant operationalcollaboration and policy bodies (such as FIRST, regional CERT bodies, the IGF, or the UN GGE), but takes mainly a passive role.	An assessment has been made of how the international debates on cybersecurity policy and related issues affect the country's interests and international standing. Specific engagement objectives have been defined accordingly. Multiple stakeholders have been involved in this process.The country is actively participating in relevant international bodies and forums, either directly or through relevant representative bodies.Their voices are being heard and are having an impact.The country actively contributes to regional/ international operational collaboration and policy bodies.	The country is actively building international communitiesof interest around specific cybersecurity policy goals and promoting their adoption.The country makes a major contribution to regional/ international operational bodies and is actively involved in building capacity in third-party countries.	The country is a leading actor in building consensus, fostering inclusivity and shaping the international debates on key cybersecurity policy issues.The country is focused on the future, seeing emerging issues (around new technology or new types of threat), and is initiating new international debates around the key issues.The country is actively involved in creating new regional/ international collaboration mechanisms.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.2 Factor - D 1.2: Incident Response and Crisis Management

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Identification and Categorisation of Incidents	No process for identifying and categorising national-level incidents exists.	Some organisations and sectors have internal mechanisms for identifying and categorising incidents within their purview.A process for identifying national-level incidents is under development.There is no central registry in place but *ad-hoc* arrangements exist for dealing with the most significant events.	Most major organisations have internal mechanisms for identifying and categorising incidents.A central registry of national- level cybersecurity incidents exists and a process for timely escalation of incidents, from the organisational to the national level, is in place.Individual national incidents are categorised according to severity and resources are allocated accordingly.	Insights arising from national level incidents are routinely analysed in order to establish lessons and inform broader cybersecurity policy and strategy.	The criteria for categorising incidents are sufficiently flexible to cater for rapidly emerging changes in the underlying technological or threat environment.The country is contributing to international best practice in incident identification and categorisation.
Organisation	No organisation for national-level cyber incident response exists.A few organisations may have internal cybersecurity response mechanisms in place but co- ordination is minimal.	A national CERT might exist but lacks sufficient resources and skills.Processes for managing incidents are still in development.Some organisations from public and private sectors have internal cybersecurity response mechanisms in place but co- ordination with the national CERT is *ad hoc*.The role of sub-national bodies is unclear.Bilateral co-operation with international partners is limited or *ad hoc*.	A national body for incident response has been established. It has the resources, skills, documented processes and legal authorities required to address the range of cyber incidentscenarios that the country is likely to face (including out-of-hours capability, if appropriate).Relationships and protocols are in place to enable incident management co-ordinationbetween the national body and other elements of the public and private sectors.The role of sub-national bodies in incident response is clear and mechanisms are in place toenable co-ordination between the national and sub-national levels.There is regular sharing of threat and vulnerability information, and operational good practices between the national body and a wide range of public and private sector organisations, as well as international partners.	The national body undertakes a wide range of engagement activities such as conveningcommunities of interest, running cross-sector exercises and promoting best cybersecurity practices.The national body innovates to provide a range of additional services that improve the country's ability to prevent, detect, respond and recover from threats.The national body is widely recognised as an authoritative voice on cybersecurity within the country.The effectiveness of the national body in reducing cyber risk and harm is regularly evaluatedand benchmarked against international good practice.	The government's overall operational response is adaptive to changes in the underlying technical and threat environment.The country is contributing to international best practice on how to organise operational responses to cybersecurity threats.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Integration of Cybersecurity into National Crisis Management	No framework exists for national- level crisis management.Cybersecurity has not been considered as a potential national-level crisis scenario.Emergency communication capabilities are limited.	A national crisis management framework is in development and a specific organisation has been allocated responsibility for leading national-level crisis response.Cybersecurity has been recognised as relevant to national crisis management, both as a factor in its own right and as an element of other crisis scenarios.An exercise programme is in development and includes cybersecurity-based scenarios.Emergency communication capabilities are in place but may not be well integrated or lack resilience to cyber disruption.	Cybersecurity is fully integrated into the national crisis management framework and the organisation responsible for crisis management is equipped to deal with a range of cybersecurity- related scenarios.The role of a cyber incident management authority within the crisis management process is well defined and established, and escalation thresholds are fully understood.National crisis management scenarios with cybersecurity components are regularly exercised.Emergency communication systems are regularly tested for cyber resilience against a range of cybersecurity-related scenarios.	Lessons learnt from cyber crisis exercises are used to inform both national crisis management policy and the national cybersecurity strategy and implementation plan.International crisis planning and exercising with partners exists and routinely includes cybersecurity as an element.The resilience of emergency communications has been stress-tested against a wide range of potential scenarios.	The country is contributing to the debate on the integration of cyber into national andinternational crisis management.Emergency communications capabilities are capable of operating beyond the country's border in order to support third- party countries and global crisis responses.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.3 Factor - D 1.3: Critical Infrastructure (CI) Protection

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Identification	There may be some appreciation of what constitutes a CI asset, but no formal categorisation of CI assets has been produced.	A list of general CI assets, sectors and operators has been created.	The list of CI assets has been formalised and incorporates a range of appropriate public and private sector organisations.Specific operators have been identified and are aware of their status.The list is kept up to date to reflect changes in the country's circumstances.Cross-border dependencies have been identified.	The list of CI assets is adaptive to strategic shifts in the underlying technical, social and economic environment.Interdependencies between sectors are managed.Cross-border dependencies are managed.	There is flexibility in the process for identifying CI assets to cater for rapidly emerging changes in the underlying technological or threat environment.The country is actively involved in the identification and prioritisation of global CI assets.Cross-sector and cross-border dependencies are mitigated.
Regulatory Requirements	There are no existing regulatory requirements specific to the cybersecurity of CI.	The need for baseline standards to govern CI assets isacknowledged but these are not explicitly mandated in regulation.Sector regulators do not routinely assess CI operators for compliance.	CI operators are mandated by regulation to meet appropriate cybersecurity standards (either in the form of specific cyber regulation or as part of broader regulatory requirements).Mandatory breach reporting and vulnerability disclosure requirements are in place. Formal processes are in place to evaluate CI operator compliance with regulatory standards and incident and vulnerability disclosure.	Novel approaches to regulatory supervision are being developed to improve CI cybersecurity while also facilitating effective and efficient CI service delivery.The country is promoting best practice regulatory approaches at an international level.	Regulatory frameworks are sufficiently flexible to cater for rapidly emerging changes in the underlying technological or threat environment.The country is actively involved in establishing regulatory approaches to assuring global CI.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Operational Practice	A few CI operators may be implementing goodcybersecurity practices, but this is inconsistent.	Many CI operators are implementing good cybersecurity practice.There is some self-assessment against recognised industry standards.Some informal arrangements exist for collaboration across and within sectors.	CI operators are consistently implementing recognised industry standards and the effectivenessof their cybersecurity controls are regularly assessed.Mechanisms are in place for operators to share threat and vulnerability information, best practices and lessons learned from incidents and near misses.CI operators participate fully in national incident response and crisis management planning and exercising. Mechanisms are in place for public authorities to provide information and other practical support to CI operators, both pre- and post- incident.	There is extensive collaboration among CI operators and with public authorities to develop strategies that enhance collective cybersecurity.The resilience of the critical infrastructure ecosystem as a whole has been assessedagainst a range of scenarios, and measures are in place to address systemic risks to the economy and society.	The country and its CI operators are contributing to the international debate on global critical infrastructure resilience.Experts from the regulators and CI operators are recognised internationally for their contribution to addressing global infrastructure protection challenges.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.4 Factor - D 1.4: Cybersecurity in Defence and National Security

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Defence Force Cybersecurity Strategy	The potential impact of cybersecurity on national security and defence may have been considered but has not been formally articulated.	The potential impact of cybersecurity on national security and defence has been assessed and a strategy for addressing these risks is under development.This analysis includes risks to the ability of the country's military and other national security assets to operate in a contested cyber environment.	A strategy for cybersecurity for national security and defence has been formally adopted (stand-alone or as part of a wider document).The strategy is supported by appropriate legal authorities and relevant operational doctrine and rules of engagement. These are consistent with international humanitarian law.The dependence of national security and military entities on the cybersecurity of other parts of the critical national infrastructure is understood and is addressedin the defence cybersecurity strategy.Cybersecurity considerations inform other elements of national security and defence strategy, where relevant.	Defence strategy includes appropriate considerations of deterrence.The country's defence and national security establishment (alongside other stakeholders) is actively engaged in the global debate on international humanitarian law and norms of behaviour as they relateto conflict in cyberspace. Declaratory strategy and published doctrine may be part of this.	Strategy and doctrine are not static but are adaptive tochanging capabilities and to the geo-political and technical threat environment.The strategy is designed to promote stability in cyberspace. This includes measures to predict and influence the strategies and actions and reactions of potential allies and adversaries.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Defence Force Cybersecurity Capability	Specialist cybersecurity capability within the national security establishment is limited.	Specialist cybersecurity capability requirements are understood, and relevant organisational structures have been defined.Initial steps have been taken to establish these.	Capabilities and organisational structures are in place and have been tested. Resourcing is provided through the national military estimate or equivalent process.Operational doctrine and rules of engagement are fully embedded in training.Specialist intelligence resources are being applied to provide support and are appropriately resourced.Mechanisms to facilitate collaboration with allies are in place and have been tested.	Relevant deterrence and defence/resilience capabilities are in place, forming part of the country's defence cybersecurity strategy.Cybersecurity is embedded in wider operational and command training within the country's military forces.	Defence cybersecurity capabilities are able to support multilateral responses to shared national security challenges.
Civil Defence Co-ordination	Collaboration on cybersecurity between civil and defence entities is limited.	Informal collaboration on cybersecurity between civil and defence entities may exist but has not been formalised.Defence entities have not been formally resourced to undertake this work.	Collaboration on cybersecurity between civil and defence entities exists and has been formalised.Respective roles have been defined within the country's crisis management procedures.The resources required within the defence and national security community, to support civil and CI authorities, have been formally assessed and assigned.Formal mechanisms are in place to determine military/ national security cybersecurity dependencies on civil and CI infrastructure. The ability of civiland CI infrastructure operators to provide these services has been assured.	Civil defence collaboration on cybersecurity is built into the strategic planning of both sectors and designed to address a range of future crisis scenarios.Mechanisms are in place that enable defence and the national security community to draw on the skills and capabilities of the broader economy and society. (For example, via a formal cyber reserve force)	The country is leading the international debate on best practice in cross-governmental, civil-defence cybersecurity collaboration.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.5 Factor - D 2.1: Cybersecurity Mindset

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Awareness of Risks	The government has minimal or no level of awareness of cybersecurity risks.The private sector has minimal or no level of awareness of cybersecurity risks.Users have minimal or no level of awareness of cybersecurity risks.	Leading government agencies have a minimal level of awareness of cybersecurity risks.Leading private firms have a minimal level of awareness of cybersecurity risks.A limited proportion of Internet users have awareness of cybersecurity risks.	There is widespread awareness of cybersecurity risks within most government agencies.There is widespread awareness of cybersecurity risks within most private firms.A growing number of Internet users within society have awareness of cybersecurity risks.	Government agencies across all levels are aware of cybersecurity risks and proactively anticipating new risks.Private sector actors at all levels are fully aware of cybersecurity risks and are anticipating new risks.Users are fully aware of cybersecurity risks and try to anticipate new risks.	Government agencies at all levels are fully aware of cybersecurity risks and use them to update cybersecurity policies and operational practices.Most private sector actors across all levels mitigate cybersecurity risks and use them to update cybersecurity policies and operational practices.Most users identify and anticipate cybersecurity risks and try to adapt their behaviour.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Priority of Security	The government has minimal or no recognition of the need to prioritise cybersecurity.Private sector actors have minimal or no recognition of the need to prioritise cybersecurity.Users have minimal or no recognition of the need to prioritise cybersecurity.No surveys or metrics exist to document cybersecurity ingovernment, private sector, or across users.	Leading government agencies and private firms recognise the need to prioritise cybersecurity.Private firms recognise the need to prioritise cybersecurity.A limited proportion of Internet users recognise the need to prioritise cybersecurity.Surveys and metrics to assess knowledge of cybersecurity within the nation are limited or *ad hoc*.	Most government agencies at all levels are making cybersecurity a priority.Most private firms at all levels are making cybersecurity a priority.A growing number of Internet users within society make cybersecurity a priority.Surveys and metrics to evaluate knowledge of cybersecurity within the nation are available.	Government agencies across all levels routinely prioritise and reassess cybersecurity priorities in response to changing threats to the population.Most private sector actors across all levels routinely prioritise and reassess cybersecurity priorities in response to changing threats to the population.Most users routinely prioritise cybersecurity and seek to take proactive steps to improve cybersecurity.Surveys and metrics are routinely conducted and publicised in fields of government, business and industry, and among users.	Government agencies at all levels habitually, as a matter of course, prioritise cybersecurity.Private sector actors at all levels habitually prioritise cybersecurity, as a matter of course.Users habitually prioritise cybersecurity and take steps to improve their security online.Survey results and metrics are used to refine cybersecurity policies, inform operational practices and IT-related initiatives within the nation.
Practices	The government agencies do not follow safe cybersecurity practices.Private sector companies do not follow safe cybersecurity practices.In this country, very few Internet users follow safe cybersecurity practices or take protective measures to ensure their security.	Leading government agencies follow safe cybersecurity practices.Leading private firms follow safe cybersecurity practices.A limited but growing proportion of Internet users know or follow safe cybersecurity practices.	Most government agencies at all levels follow safe cybersecurity practices.Most private firms at all levels follow safe cybersecurity practices.Most Internet users within this country know and follow safe cybersecurity practices	Government agencies across all levels routinely follow safe cybersecurity practices.Most private sector actors, (including SMEs) across all levels routinely follow safe cybersecurity practices.Most users know and routinely follow safe cybersecurity practices.	Government agencies at all levels habitually follow and also develop safe cybersecurity practices.Private sector actors at all levels habitually follow and develop safe cybersecurity practices.Nearly all users know and habitually follow safecybersecurity practices as a matter of course.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.6 Factor - D 2.2: Trust and Confidence in Online Services

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Digital Literacy and Skills	Very few Internet users in this country critically assess what they see or receive online.Internet users generally do not believe or even consider that they have the ability to use the Internet and protect themselves online.No programmes are available to support digital and media literacy skills.	A limited but growing proportion of Internet users critically assess what they see or receive online.A limited proportion believe that they have the ability to use the Internet and protect themselves online.One or more programmes are being developed to support digital and media literacy skills.	Most Internet users critically assess what they see or receive online, based on identifying possible risks.Most Internet users understand how and act to protect themselves from misinformation online, such as performing a search.Programmes have been developed to support digital and media literacy skills.	Most Internet users critically assess what they see or receive online, based on identifying possible risks.Most Internet users recognise questionable information online and take steps to ignore it or check its validity.Efforts are under way to co-ordinate programmes that support Internet, digital, and media literacy skills between Internet platform providers, regulators and civil society.	Nearly all Internet users habitually assess the risk in using online services, including changes in the technical and cybersecurity environment.Internet users continuously adjust their behaviour based on their assessments of the quality of information they receive.Internet platform providers, regulators and civil society are collaboratively developingprogrammes to support Internet, digital, and media literacy skills.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
User Trust and Confidencein Online Search and Information	Most Internet users have no trust or have a blind trust in websites and what they see or receive online.Very few Internet users feel confident in using the Internet.Surveys or other metrics to assess users' trust and confidence online are not available.	Only a limited proportion of users have sufficient trust in their use of the Internet.A limited proportion of Internet users feel confident using it.Surveys and metrics to assess users' trust and confidence online are limited or *ad hoc*.	A growing proportion of users have sufficient trust in using the Internet safely and recognise indicators of legitimate sites and information sources.A growing number of users feel confident using the Internet.Surveys and metrics to assess users' trust and confidence online are in place and adequately funded.	Most users have a learned level of trust in using the Internet safely and recognise indicators of legitimate sites and information sources.Most Internet users feel confident using the Internet, believe they can recognise problematic or non-legitimate websites (including mimicry attempts), and check information using tools such as search options. Surveys and metrics to assess users' trust and confidence online are routinely conducted.	Nearly all users trust that they can safely use of the Internet for a variety of purposes and can help others to use it safely.Nearly all Internet users feel confident using the Internet and sourcing valid content.Surveys and metrics have a strong reputation in the region or globally and are shaping the development of metrics in other nations.
Disinformation	Internet platform providers are not addressing issues of disinformation such asmisinformation, in this nation.Civil society and other non-government actors lack the tools and resources to address online disinformation, suchas exposing misinformation campaigns.Government agencies and actors have not addressed online disinformation online.	Internet platform providers are developing approaches toaddress issues of disinformation in this nation.The development of tools and resources to address disinformation have beeninitiated by leading civil society and non-governmental actors.Government programmes and initiatives to address disinformation are beingdeveloped but entail filtering and limited efforts to inform Internet users.	Internet platform providers have a number of approaches in place to address disinformation; theserespect freedom of expression and other human rights online.Civil society stakeholders have developed tools and resources to address online disinformation.Government programmes and initiatives to strengthen the public's preparedness against online disinformation are restricted to awareness raising, but avoid censorship or filtering of information.	Internet platform providers have instituted policies and practices to address disinformation; these respect freedom of expression and other human rights online.The joint efforts of civil society stakeholders are in place and are regularly used to address online disinformation in ways that respect freedom of expression and other human rights online.Outcome-oriented surveys are used to refine programmes and initiatives aimed at empowering users and building the public's understanding of possible online disinformation.	Internet platform providers have instituted policies and practices to address disinformation in some innovative ways that respect freedom of expression and other human rights online.The joint efforts of civil society stakeholders are proactively reviewed to take account of broader strategic developments related to disinformation and awareness raising.The country is supporting the development of national/ regional/ international action plans and guidelines to address disinformation in ways that protect an open Internet and empower users.
User Trust inE-government Services	Government offers a very limited number of e-services, if any, and has not publicly promoted their security.Generally, the public does not use any significante-government services.No surveys or metrics exist to show how Internet users trust e-government services.There is a lack of information about e-government security and security breaches.	Government has begun to build a core set of e-services, for which they recognise the need to apply security measures in order to establish trust in their use.A limited number of early adopters trust in the secure use of e-government services.Metrics to assess users' trust in e-government services is limited or *ad hoc*.Public authorities are developing information on privacy and security initiatives and breaches in an *ad-hoc* manner.	Key e-government services have been developed and have generated a large number of users.A sizeable and growing number of Internet users trust in the use of e-government services.Surveys and metrics to assess users' trust in e-government services are in place and adequately funded.Public authorities are publishing information and updates of their privacy and security breaches and initiatives such as privacy by default.	E-government services have become the dominant (default) mode of government information service delivery.The majority of Internet users in this country trust in the secure use of e-government services and make use of them.Surveys and metrics to assess users' trust in e-government services are routinely conducted.Public authorities are co- ordinating, publishing and informing users about privacy and security initiatives and breaches.	E-government services in this country are recognised regionally or internationally.Internet users trust thate-government services are proactively reviewed, improved and expanded to enhance their security.Outcome-oriented surveys are used to review e-government services and evaluate the management of online content.The country is a leader in informing users about current and developing privacy and security breaches, initiatives and other issues.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
User Trust in E-commerce Services	E-commerce services are not offered.Internet users lack the trust to use any available e-commerce services.No surveys or metrics exist to show how Internet users trust e-commerce services.There is little or no recognition of the need for security initiatives for e-commerce services.	E-commerce services are being provided to a limited extent.A limited number of early adopters trust in the secure use of e-commerce services.Metrics to assess users' trust in e-commerce services is limited or *ad hoc*.The private sector recognises the need for the application of security measures to establish trust in e-commerce services.	E-commerce services are fully established by multiple stakeholders in a secure environment.A sizeable and growing number of Internet users trust in the secure use of e-commerce services.Surveys and metrics to assess users' trust in e-commerce services are in place and adequately funded.Reliable security solutions are up to date and available, such as for payment systems. Certification schemes and trust marks fore-commerce services are in place.	E-commerce services have become widely accepted as a safe practice for consumers.The majority of users trust in the secure use of e-commerce services and make use of them.Surveys and metrics to assess users' trust in e-commerce services are routinely conducted.Stakeholders are investing in enhanced service functionality of e-commerce services, protection of personal information andthe provision of user feedback mechanisms.	E-commerce services in this country are recognised regionally or internationally.Internet users trust that e-commerce services areproactively reviewed, improved and expanded to enhance their security.Outcome-oriented surveys are used to review and improvee-commerce services in order to promote transparent,trustworthy and secure systems.Terms and conditions provided by e-commerce services are clear and easily comprehensible to all users.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.7 Factor - D 2.3: User Understanding of Personal Information Protection Online

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Personal Information Protection Online	Users and stakeholders within the public and private sectors have no or minimal knowledge about how personal information is handled online, nor do they believe that adequate measures are in place to protect their personal information online.There is no or limited discussion regarding the protection of personal information online.Privacy standards are not in place to shape Internet and social media practices.	Users and stakeholders within the public and private sectors may have general knowledge about how personal information is handled online; and may employ good (proactive) cybersecurity practices to protect their personal information online.Discussions have begun regarding the protection of personal information and about the balance between security and privacy.Concrete actions or privacy policies are being developed.	A growing proportion of users have the skills to manage their privacy online, and protect themselves from intrusion, interference, or unwanted access of information by others.There is considerable public debate regarding the protection of personal information and about the balance between security and privacy.Privacy policies have been developed within the public and private sectors.	All stakeholders have the information, confidence and the ability to take steps to protect their personal information online and to maintain control of the distribution of this information.Users and stakeholders within the public and private sectors widely recognise the importance of protection of personal information online and are aware of their privacy rights.Mechanisms are in place in private and public sectors to shape Internet and social media practices and ensure that privacy and security do not compete.	Users have the knowledge and skills necessary to protect their personal information online, adapting their abilities to the changing risk environment.Policies in private and public sectors are proactively reviewed to ensure privacy and security do not compete in a changing environment and are informed by user feedback and public debate.New mechanisms are in place, such as privacy by default, as tools for transparency and are promoted.

B.3.8 Factor - D 2.4: Reporting Mechanisms

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Reporting Mechanisms	There are no official reporting mechanisms available, but discussions might have begun.Users do not use social media channels to raise concerns over any cyber harms and problems.No metrics of reported incidents exist.	The public and/or private sectors are providing some channelsfor reporting cyber harms (such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents), but these channels are not co-ordinated and are used in an *ad-hoc* manner.Internet users use social media channels to inform other users in an *ad-hoc* manner.Metrics of reported incidents is being developed.	Reporting mechanisms have been established, promoted and are regularly used.Internet users widely use social media channels to inform other users.There are good metrics of reported incidents.	Co-ordinated reporting mechanisms are widely used and promoted within public and private sectors.Internet users routinely use social media channels to inform other users.Cyber harm metrics have been used to inform the revision and promotion of new policies and practices.	Mechanisms have been developed to co-ordinate response to reported incidents between law enforcement and the national incident response capability.Internet users habitually use social media channels to inform other users and share good practice.Metrics are routinely used to inform policy and decision- makers.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.9 Factor - D 2.5: Media and Online Platforms

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Media and Social Media	Mass media rarely, if ever, cover information about cybersecurity or report on issues such as security breaches or cybercrime.There is no, or rarely any discussion on social media about cybersecurity.Any portrayal of whistleblowers is negative, and based on criminal or other negative stereotypes.	It is perceived that there is *ad-hoc* mass media coverage of cybersecurity, with limited information provided andreporting on specific issues that individuals face online, such as protection for children online, or cyber-bullying.It is perceived that there is limited discussion on social media about cybersecurity.There have been positive examples of cases where whistleblowers have had a constructive impact.	It is perceived that cybersecurity is a common subject across mainstream media, and information and reports on a wide range of issues, including security breaches and cybercrime, are widely disseminated.There is broad discussion on social media about cybersecurity.There is acceptance that whistleblowers can play a positive role.	It is perceived that mass media coverage extends beyond threat reporting and can inform the public about proactiveand actionable cybersecurity measures, as well economic and social impacts.There is frequent discussion on social media about cybersecurity and individuals regularly use social media to share online experiences.Transparency is encouraged as are whistleblowers.	It is perceived that the broad discussion of personal experiences and personalattitudes of individuals across mainstream and social media inform policy making and facilitate societal change.Social media has become a major component in tracking and addressing cyber harms.Whistleblowing has been encouraged and protected as a means of social accountability.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.10 Factor - D 3.1: Building Cybersecurity Awareness

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Initiatives by Government	No overarching national cybersecurity awareness-raising programme has been developed by the government.The need for awareness of cybersecurity threats and vulnerabilities in the government is not recognised or is only at initial stages of discussion.	A co-ordinated cybersecurity awareness raising programme with the involvement ofthe government is under development, with relevant stakeholders involved, including the private sector and civil society.Awareness-raising programmes, courses, seminars and online resources initiated by the government are available but not sufficiently reflected in thenational cybersecurity strategy or is in development.The actions within the programmes are led by different 'owners' but they are not yet co- ordinated.The availability of adequate resources has not yet been confirmed.Initial system of mechanisms and metrics to review processes are limited or *ad hoc*.	A co-ordinated national cybersecurity awareness- raising programme with detailed implementation plan is published. The contentincludes explicit links to national cybersecurity strategy.A co-ordinating body has been assigned with sufficient authority and resources required to deliver the actions of the national programme.A national cybersecurity awareness portal exists to improve the skills and knowledge of the societyand is disseminated via that programme.Programme review processes and outcome-oriented metrics are in place, are adequately funded and allow effectiveness to be measured.	The national awareness-raising programme is fully integrated with sector-specific, tailored awareness-raising programmes, such as those focusing on industry, academia, civil society, and/or women and children.Emerging cybersecurity risks are regularly assessed and used to update the nationalcybersecurity awareness-raising programme.There is evidence of these metrics being used to refine actions within the national awareness-raising programme and national cybersecurity strategy.	The national cybersecurity awareness-raising programme with private and civil society stakeholders is proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental).The country is actively involved in creating new regional/ international cybersecurity awareness-raising programmes that contribute toward expanding and enhancing international awareness-raising good practices.The national cybersecurity awareness-raising programme has a measurable impact on the reduction of the overall threat landscape.
Initiatives by Private Sector	The need for awareness of cybersecurity threats and vulnerabilities in the private sector is not recognised or is only at initial stages of discussion.	Awareness-raising programmes, courses, seminars and online resources initiated by the private sector are available but no co-ordination or scaling efforts have been conducted.Initial system of mechanisms and metrics to review processes are limited or *ad hoc*.	Collaborative awareness-raising efforts (e.g.: joint policy and/or advocacy work) with government and civil society stakeholdersare made in order to pool resources, information and identify solutions for cyber safety practices.The role of specific 'owners' assigned to actions within private sector initiatives are clear and mechanisms are in place to enable co-ordination between the levels of government, private sector and civil society.Programme review processes and outcome-oriented metrics are in place, well-funded and shared with government and civil society stakeholders.	The effectiveness of joint awareness-raising efforts with government and civil society stakeholders is regularly assessed and used to enhance collaborative processes.Private sector initiatives are fully integrated into the national awareness-raising programme.Evidence from the lessons learnt is fed into the development of future programmes.	The joint awareness-raising efforts with government and civil society stakeholders are proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental).The joint awareness-raising efforts with government and civil society stakeholders have a measurable impact on reduction of the overall threat landscape.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Initiatives by Civil Society	The need for awareness of cybersecurity threats and vulnerabilities in civil society is not recognised or is only at initial stages of discussion.	There are indications that civil society realises that it can play a role in awareness-raising programmes, courses, seminarsand online resources, but no real deliverables are yet evident.Initial system of metrics may exist.	Collaborative awareness-raising efforts (e.g.: joint policy and/or advocacy work) with government and private sector stakeholders are taking place in order to pool resources and information and identify solutions for cyber safety practices.The role of specific 'owners' assigned to actions within civil society initiatives are clear and mechanisms are in place to enable co-ordination between the levels of government, private sector and civil society.Programme review processes and outcome-oriented metrics are in place, well-funded and shared with government and private sector stakeholders.	The effectiveness of joint awareness-raising efforts with government and privatesector stakeholders is regularly assessed and used to enhance collaborative processes.Civil society initiatives are fully integrated into the national awareness-raising programme.Evidence from the lessons learnt is fed into the development of future programmes.	The joint awareness-raising efforts with government and private sector stakeholders are proactively reviewed to take account of broader strategic developments within the country (political, economic, social, technical, legal and environmental).The joint awareness-raising efforts with government and private sector have a measurable impact on reduction of the overall threat landscape.
Executive Awareness Raising	Awareness raising on cybersecurity issues for executives is limited or non-existent.Executives are not yet aware of their responsibilities toshareholders, clients, customers, and employees in relation to cybersecurity.	Executives are made aware of general cybersecurity issues, but not how these issues and threats might affect their organisations.Executives of particular sectors, such as finance andtelecommunications, have been made aware of cybersecurity risks in general, and howthe organisation deals with cybersecurity issues, but not of strategic implications.	Awareness raising of executives in the public, private, academic and civil society sectors address cybersecurity risks in general, some of the primary methods of attack, and how the organisation deals with cyber issues (usually abdicated to the CIO).Select executive members are made aware of how cybersecurity risks affect the strategic decision making of the organisation, particularly those in the financial and telecommunications sectors.Awareness-raising efforts of cybersecurity crisis management at the executive level is still reactive in focus.	Executive awareness-raising efforts in nearly all sectors include the identificationof strategic assets, specific measures in place to protect them, and the mechanism by which they are protected.Executives are able to alter strategic decision making and allocate specific funding and people to the various elements of cyber risk, contingent on their company's prevailing situation.Executives are made aware of what contingency plans arein place to address various cyber-based attacks and their aftermath.Executive awareness courses in cybersecurity are mandatory for nearly all sectors.	Cybersecurity risks are considered as an agenda item at every executive meeting, and funding and attention is reallocated to address those risks.Executives at regional and international level are regarded as a source of good practice in responsible and accountable corporate cybersecurity governance.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.11 Factor - D 3.2: Cybersecurity Education

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Provision	Few or no cybersecurity educators are available, and there are no qualification programmes for educators.Computer science courses are offered that may have a security component, but nocybersecurity-related courses are offered.No accreditation in cybersecurity education exists.	Qualification programmes for cybersecurity educators are being explored, with a small cadre of existing qualified educators.Some educational courses exist in cybersecurity-related fields, such as information security, network security and cryptography, but cybersecurity-specific courses are not yet offered.A demand for cybersecurity education is evidenced through course enrolment and feedback.	Qualifications for and supply of educators are readily available in cybersecurity.Specialised courses in cybersecurity are offered and accredited at university level.Cybersecurity risk-awareness modules are offered as part of many university courses.Degrees in cybersecurity-related fields are offered by universities or equivalent educational institutions.Universities and other bodies hold seminars/lectures on cybersecurity issues, aimed at non-specialists.Research and development are leading considerations in cybersecurity education.Cybersecurity education is not limited to universities or equivalent educationalinstitutions, but ranges from primary, secondary and tertiary to post-graduate levels, including vocational education.Steps might have been taken to incorporate STEM orequivalent education framework with a focus on cybersecurity throughout primary and secondary curricula.	Cybersecurity educators are not only drawn from the academic environment, but incentives are in place so that industry and/or government experts take these positions as well.Accredited cybersecurity courses are embedded in all computer science degrees.Degrees are specifically offered in cybersecurity, and encompass courses and models in various other cybersecurity-related fields, including technical and non-technical elements such as policy implications, and multi-disciplinary education.Cybersecurity educational offerings are weighted and focused on an understanding of current risks and skills requirements. The content of cybersecurity courses covers topics on emerging threats in cybersecurity.National or international cybersecurity frameworks and/ or curricular guidelines are taken into consideration by academic institutions when designing cybersecurity courses.Apprenticeship programmes in different industry sectors are offered to combine knowledge and practical skills.	National courses, degrees, and research are at the forefront of cybersecurity education.Cybersecurity education programmes maintain a balance between preserving core components of the curriculum and promoting adaptive processes that respond to rapid changes in the cybersecurity environment.Prevailing cybersecurity requirements are considered in the redevelopment of all general curricula.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Administration	The need to enhance national cybersecurity education is not yet considered.A network of national contact points for governmental, regulatory bodies, critical industries and education institutions is not yet established.Discussion of how co-ordinated management of cybersecurity education and research enhances national knowledge development has not or has only just begun.	The need to enhance cybersecurity education in schools and universities or equivalent educationalinstitutions has been identified by leading government, industry, and academic stakeholders.Schools, government and industry collaborate in an*ad-hoc* manner to supply the resources necessary for providing cybersecurity education.A national budget focused on cybersecurity education is not yet established.Initial system of mechanisms and metrics to review the supply and demand for cybersecurity courses are limited or *ad hoc*.	Broad consultation across government, private sector, academia and civil society stakeholders informs cybersecurity education priorities and is reflected in national cybersecurity strategy.National budget is dedicated to national cybersecurity research and laboratories at universities or equivalent educational institutions.Competitions, initiatives and funding schemes for students and employees are promoted by government and/or industry in order to increase the attractiveness of cybersecurity careers.Programme review processes and outcome-oriented metrics to review the supply and demand for cybersecurity courses are in place and well-funded.	Metrics are being used to refine actions within educational investment to create a cadreof cybersecurity experts in the country across, all sectors.Management of the government budget and spending on cybersecurity education is based on national demand.Leading national cybersecurity academic institutions share lessons learnt with other national and international counterparts.Government has established academic centres of excellence in cybersecurity.	International cybersecurity centres of excellence are established through twinning programmes led by world-class institutions.Co-operation between all stakeholders in cybersecurity education is routine and can be proven.Content in cybersecurity education programmes is aligned with practical cybersecurity problems and business challenges and provides a mechanism for enhancing curricula based on the evolving landscape.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.12 Factor - D 3.3: Cybersecurity Professional Training

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Provision	Few or no training programmes in cybersecurity exist.	The need for training professionals in cybersecurity has been documented at the national level.Training for general IT staff is provided on cybersecurity issues so that they can react to incidents as they occur, but no training for dedicated security professionals exists.ICT professional certification is offered, with some security modules or components.Best practice training and certifications might be accessible via international online sources (e.g.: CISSP).*Ad-hoc* training courses, seminars and online resources are available for cybersecurity professionals through public or private sources, with limited evidence of take-up.	Structured cybersecurity training programmes exist to develop skills towards building a cadre of cybersecurity- specific professionals.National or international cybersecurity vocational-based frameworks and international best practices are taken into consideration when designing professional training courses.Security professional certification is offered across sectors within the country.The needs of society are well understood, and a list of training requirements is documented.Training programmes for non-cybersecurity professionals are recognised and offered.Government initiatives to stay in the country after the successful completion of cybersecurity training programmes might be in place.	A range of cybersecurity training courses is tailored towards meeting national strategic demand and aligns with international good practice.The training programmes outline the priorities in the national cybersecurity strategy.Training programmes are offered to cybersecurity professionals and focus on the skills necessary to communicate technically complex challenges to non- technical audiences, such as management and general employees.Outcome-oriented metrics drawn from comprehensive supply-and- demand data for cybersecurity professionals are being used to inform the modes, sustainability and procedures of future training programmes.	The public and private sector collaborate to offer training, and constantly adapt and seek to build skillsets drawn from both sectors.Training offerings and education programmes are co-ordinated so that the foundation established in schools can enable training programmes to build a highly skilled workforce.Programmes and incentive structures are in place to ensure the retention of the trained workforce within the country.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Uptake	Training uptake by IT personnel designated to respond to cybersecurity incidents is limited or non-existent.There is no transfer of knowledge from employees trained in cybersecurity to untrained employees.	Metrics that evaluate the take- up of *ad-hoc* training courses, seminars, online resources, and certification offerings are limited in scope or *ad hoc*.The transfer of knowledge from employees trained in cybersecurity to untrainedemployees in both the public and private sectors is *ad hoc*.	There is an established cadre of certified employees trained in cybersecurity issues, processes, planning and analytics.A national register of successful and certified students and professionals might exist.The transfer of knowledge from employees trained in cybersecurity to untrained employees in both public and private sectors is established.Job creation initiatives for cybersecurity within organisations are established and encourage employers to train staff to become cybersecurity professionals.Programme review processes and metrics are in place to allow progress to be measured and assess the supply and demand for cybersecurity-skilled workers in both public and private environments. These processes are adequately funded.	The uptake of cybersecurity training is used to inform future training programmes.Co-ordination of training across all sectors ensures the national demand for professionals is met.	Cybersecurity professionals not only fulfil national requirements, but domestic professionals overseas are consulted to share lessons learnt and best practice.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.13 Factor - D 3.4: Cybersecurity Research and Innovation

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
	There are limited or no cybersecurity research and development (R&D) activities occurring in the country.There is no access to R&D activities in cybersecurity from other countries.	Some integration of cybersecurity R&D activities occurs within the country, or with a partner country that understands how cyberactivity R&D applies to the local context of the country.The country may participate in relevant regional/ international cybersecurity-related research collaboration networks.	Cybersecurity R&D activities have been established and are indicated in the national cybersecurity strategy. R&D strategy may be in development.The resources and processes required to deliver the actions of cybersecurity R&D activities have been identified and are in place. Funding is adequate to deliver these actions.	The country is actively building communities of interest around R&D priorities in cybersecurity.R&D strategy is in place and fully implemented.The country makes a major contribution to cybersecurity R&D and is actively involved in building innovation capacity through international R&D consortia and investment.	The country is a leading actor in cybersecurity research and innovation and is shaping international debates on the development of R&D strategic plans.The country is forward looking, seeing emerging issues (around new technology or new types of threat), and uses R&D to prepare a future threat environment.

Research and Development		Cybersecurity R&D performancemetrics are limited in scope, or*ad hoc*.	There is active regional/international collaboration with leading practice and developments.The country is actively participating and contributing to regional/ international cybersecurity-related research collaboration networks.Metrics for measuring R&D performance are in place and allow progress to be measured and to improve the cybersecurity R&D capability of the country.	Emerging cybersecurity risks are regularly assessed and used to update the national cybersecurity strategy and the development of future programmes of the R&D strategy.Synergy between academic institutions and industry supports R&D activities and is used to design cyber curricula that cover industry needs.	The country is contributing to international best practices in cybersecurity R&D.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.14 Factor - D 4.1: Legal and Regulatory Provisions

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Substantive Cybercrime Legislation	Specific substantive criminal law on cybercrime does not exist. General criminal law may exist, but its application to cybercrime is unclear.	Partial legislation exists that addresses some aspects of cybercrime, or cybercrime legal provisions are in development.	Substantive cybercrime legal provisions are contained in specific legislation or a general criminal law.The country may have ratified regional or international instruments on cybercrime. The country consistently seeks to implement these measures into domestic law.	Measures are in place to exceed minimal baselines specified in international treaties, where appropriate.The country seeks to adapt its substantive cybercrime legislation to take account ofemerging technologies and their use.	Substantive cybercrime law is constructed so that it can cater for dynamic changes inthe underlying technology and threat environment, without the need for substantial and lengthy revision.The country is actively contributing to the international promotion of effective cybercrime legislation.
Legal and Regulatory Requirements for Cybersecurity	There are limited cybersecurity requirements set out in regulation or law.The need to create legal and regulatory frameworks on cybersecurity may have been recognised and may have resulted in a gap analysis.	Stakeholders from relevant sectors have been consulted to support the establishment of legal and regulatory frameworks.Draft legislation and regulation may be in place, but this has yet to be adopted and may not cover all relevant sectors.	Comprehensive cybersecurity requirements are set out in relevant regulation and law (including sector-specific requirements, where relevant).These requirements may include mandatory standards, or breach notification requirementsand vulnerability disclosure requirements.Relevant civil and criminal liabilities are clearly articulated and understood by regulated entities.Relevant legal and regulatory bodies have the powers needed to enforce these requirements.	The effectiveness of law and regulation in improvingcybersecurity practice is regularly assessed and used to inform their future development.Regulations are updated to take account of emerging technologies.	Regulatory frameworks are sufficiently flexible to cater for rapidly emerging changes in the underlying technological or threat environment.The country is promoting best practice legal and regulatory approaches internationally.The country is actively involved in the development of international agreements to promote harmonisation and mutual recognition of cybersecurity laws and regulations.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Procedural Cybercrime Legislation	Specific procedural criminal law for cybercrime does not exist. It is not clear how general criminal procedural law applies to cybercrime investigations, prosecutions, and electronic evidence.	Development of specific procedural cybercrime legislation, or amendment of general procedural criminal law to adapt to cybercrime cases, has begun.	Comprehensive criminal procedural law containing provisions on the investigation of cybercrime and evidentiary requirements has been adopted and is applied.The country may have ratified regional or international instruments on cybercrime. The country consistently seeks to implement these measures into domestic law.Procedural laws relating to cybercrime permit the exchange of information (and other actions required) to support successful cross-border investigation of cybercrime.	Measures are in place to exceed minimal baselines specified in international treaties, where appropriate.The country seeks to adapt procedural cybercrime legislations to take account of emerging technologies and their use.	Procedural cybercrime law is constructed in a way that it can cater for dynamic changes in the underlying technology andthreat environment, without the need for substantial and lengthy revision.The country is actively contributing to the promotion of effective procedural cybercrime legislation and instruments to improve international cybercrime investigations.
Human Rights Impact Assessment	Substantive and procedural cybercrime legislation and cybersecurity regulations may be in development, but no human rights impact assessments have been carried out.	Human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations may have been conducted, including consideration of privacy and freedom of expression implications. Some issues, however, have yet to be resolved.Relevant human rights experts have been consulted in the development of the legislation and regulation.	Full human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations have been completed and international standards are met.Implementation of this legislation is monitored on a regular basis for human rights compliance, and this is independently verified.	Human rights impact assessments are regularly reviewed to ensure that practice remains compatible with human rights requirements, and that the effect of emerging technologies is considered.Consideration has also been given to how cybersecurity can enhance human rights protection within the country and internationally.	The country is actively contributing to the development and promotion of human rights impact assessments as they relate to cybersecurity.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.15 Factor - D 4.2: Related Legislative Frameworks

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Data Protection Legislation	Data protection legislation does not exist.	Data protection legislation is in development.Stakeholders from relevant sectors have been consulted to support the development of this legislation.	Comprehensive data protection legislation in line with international standards and best practice has been adopted and is enforced.A lead agency responsible for data protection has been designated.	The effectiveness of data protection legislation is regularly assessed and used to inform its development.The country seeks to adapt data protection laws to take account of emerging technologies and their use.	Data protection legislation is constructed so that it cancater for dynamic changes in the underlying technology andthreat environment, without the need for substantial and lengthy revision.The country is developing and promoting international standards for data protection legislation.The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Child Protection Online	Legislation relating to child protection is limited and its application in the online environment is yet to be considered.	Legislation related to child protection is in place and is being adapted to reflect its application in the online environment.Stakeholders from relevant sectors have been consulted to support the development and adaptation of this legislation.	The application of child protection in the online environment is understood and reflected in relevant legislation. Legislation is implemented in line with international standards and best practice.	The effectiveness of online child protection law is regularly assessed and used to inform its development.The country seeks to adapt child protection law to take account of emerging technologies and their use.	Online child protection law is constructed so that it can cater for dynamic changes inthe underlying technology and threat environment, without the need for substantial and lengthy revision.The country is developing and promoting international standards for online child protection law.The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.
Consumer Protection Legislation	Legislation related to consumer protection is limited andits application in the online environment is yet to be considered.	Legislation related to consumer protection is in place and is being adapted to reflect its application in the online environment.Stakeholders from relevant sectors have been consulted to support the development of this legislation.	The application of consumer protection in the online environment is understood and reflected in relevant legislation. Legislation is implemented in line with international standards and best practice.	The effectiveness of online consumer protection law is regularly assessed and used to inform its development.The country seeks to adapt consumer protection legislation to take account of emerging technologies and their use.	Consumer protection legislation is constructed so that it can cater for dynamic changes in the underlying technology andthreat environment, without the need for substantial and lengthy revision.The country is developing and promoting internationalstandards for online consumer protection law.The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.
Intellectual Property Legislation	Legislation related to intellectual property protection is limited and its application in theonline environment is yet to be considered.	Legislation related to intellectual property protection is in place and is being adapted to reflect its application in the online environment.Stakeholders from relevant sectors have been consulted to support the development of this legislation.	The application of intellectual property protection in the online environment is understood and reflected in relevant legislation. Legislation is implemented in line with international standards and best practice.	The effectiveness of online intellectual property protection law is regularly assessed and used to inform its development.The country seeks to adapt intellectual property protection legislation to take account of emerging technologies and their use.	Intellectual property legislation is constructed so that it can cater for dynamic changes in the underlying technology andthreat environment, without the need for substantial and lengthy revision.The country is developing and promoting internationalstandards for online intellectual protection law.The country is actively involved in the development of legal instruments to enable improved international collaboration in this area.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.16 Factor - D 4.3: Legal and Regulatory Capability and Capacity

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Law Enforcement	Law enforcement officers/ agencies do not have sufficient capacity to prevent and combat cybercrime and do not receive specialised training on cybercrime investigations.	Traditional investigative measures are applied to cybercrime investigations, but digital investigation capacity is limited.Law enforcement officers may receive training on cybercrime and digital evidence, but it is *ad hoc*.	A comprehensive institutional capacity with sufficient human, procedural and technological resources to investigate cybercrime cases has been established.Digital chain of custody and evidence integrity is established, including formal processes, roles and responsibilities.Standards for the training of law enforcement officers on cybercrime and digital evidence exist and are implemented.The respective roles of national and state/local law enforcement agencies are understood and state-/local-level forces are equipped to undertake their role.	Quantified risk assessments are used to allocate resources to operational cybercrime units (at national and state/local levels).Trends and statistics on cybercrime, law enforcement interventions and their impact on harm reduction are collected, analysed and used to inform strategy and long-term resource allocation decision.Law enforcement strategies include crime prevention measures alongside enforcement measures. Intelligence is used to support proactive investigation.Law enforcement agencies have the capabilities to maintainthe integrity of data to meet international evidential standards in cross-border investigation.	The country is actively involved in the development of collaborative platforms between national law enforcement authorities.The law enforcement agencies within the country are at the forefront of developing new capabilities and approaches for the prevention and disruption of cybercrime and promoting their use internationally.
Prosecution	Prosecutors do not receive adequate training and resources to review electronic evidence or prosecute cybercrime.Consultation may have begun to consider this capacity in the prosecutor community.	A limited number of prosecutors have the capacity to conduct cybercrime cases and to handle electronic evidence, but this capacity is largely *ad hoc* and is not institutionalised.If prosecutors receive training on cybercrime and digital evidence, it is *ad hoc*.	A comprehensive institutional capacity, including sufficient human and technological resources, to prosecute cybercrime cases and cases involving electronic evidence is established.A specialist cadre of cybercrime prosecutors may have been established.	Institutional structures are in place, with a clear distribution of tasks and obligations within the prosecution services at all levels of the state.A mechanism exists that enables the exchange of informationand good practices between prosecutors and judges to ensure efficient and effective prosecution of cybercrime cases.	There is national capacity to prosecute complex domestic and cross-border cybercrime cases.
Courts	There is no process to equip judges so they can preside over cybercrime cases or cases involving electronic evidence.Consultation may have begun to consider this capacity in the judicial community.	A limited number of judges have the capacity to preside over a cybercrime case, but this capacity is largely *ad hoc*.If judges receive training on cybercrime and digital evidence, it is *ad hoc*.	Sufficient human and technological resources are available to ensure effective and efficient legal proceedings regarding cybercrime cases and cases involving electronic evidence.Judges receive specialised training about cybercrime and electronic evidence.States/local courts are equipped to deal with cybercrime cases, appropriate to their level.Relevant courts are equipped to process civil litigation relating to cybersecurity liability.	The institutional capacity of the court system to conduct cybercrime cases is frequently reviewed and revised based on an assessment of effectiveness.	The country is actively involved in developing and promoting best practices in the conduct of cybercrime cases.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Regulatory Bodies	Sector-specific regulators have limited understanding of the potential impact of cyber on their regulated entities.There is no cross-sector regulatory body to supervise specific cybersecurity requirements.	Sector-specific regulators have started to establish their cybersecurity roles.A requirement for the establishment of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations may have been considered.Relevant stakeholders have been consulted in this process.	Sector-specific regulators (e.g.: finance, energy, transport) are equipped with the capability and resources required to oversee compliance with cybersecurity requirements within their sector.Where cross-sector regulatory bodies have been established to oversee cybersecurity, they have the necessary capability and resources to undertake their role.	The impact of regulatory actions on organisations' cybersecurity practices are regularly assessed and used to inform supervisory activity and regulation development.Regulatory bodies regularly assess emerging technologies and their potential impact on the cybersecurity of regulated entities.Regulatory interventions and investigations are informed by, and prioritised on the basis of, national assessments of cyber risk.	Regulatory bodies are actively involved in the development and promotion of regulatory best practice internationally.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.17 Factor - D 4.4: Formal and Informal Co-operation Frameworks to Combat Cybercrime

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Law Enforcement Co-operation with Private Sector	Co-operation between domestic public and private sectors on cybercrime is limited.Specifically, co-operation between Internet service and other technology providers and law enforcement has not been established.	Exchange of information on cybercrime between domestic public and private sectors is *ad hoc* and unregulated.Specifically, *ad-hoc* co-operation between Internet service and other technology providers and law enforcement exists but is not always effective.	Information is regularly exchanged between domestic public and private sectors and is supported by appropriate legislation.Effective co-operation mechanisms between Internet service and other technology providers and law enforcement have been established aspart of these broader public–private sector collaboration arrangements.	The effectiveness of public and private co-operation is regularly assessed and used to enhance collaborative processes.Collaboration frameworks are regularly adapted to takeaccount of new technologies and emerging forms of cybercrime.	The country is actively contributing to the promotion of public–private partnership and the development of international public–private partnership platforms.
Co-operation withForeign Law Enforcement Counterparts	There are minimal or no forms of international co-operation to prevent and combat cybercrime.	Formal mechanisms of international law enforcement co-operation may exist, but their application to cybercrime is *ad hoc* or only possible in some cases.Law enforcement is not formally integrated into regional and international cybercrime networks.	Formal mechanisms of international law enforcement co-operation have been established to facilitate the detection, investigation, and prosecution of cybercrime.Mutual legal assistance, extradition agreements and mechanisms have been established and are applied to cybercrime cases.Domestic law enforcement agencies are integrated with regional and international networks, such as Interpol or 24/7 networks.	Law enforcement agencies work jointly with foreign counterparts, potentially through joint task forces, resulting in successful cross-border cybercrime investigations and prosecutions.	The country actively contributes to the promotion and development of international co-operation mechanisms.
Government-Criminal Justice Sector Collaboration	There is minimal interaction between government and criminal justice actors.	Exchange of information between government and criminal justice actors is limited and *ad hoc*.	Formal relationships between government and criminal justice actors have been established, resulting in the regular exchange of information on cybercrime issues.	The relationship between government actors, prosecutors, judges and law enforcement agencies is regularly assessed and used to enhance their effectiveness.	The country actively contributes to the international promotion of efficient and timely exchange of information between government and criminal justice actors.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.18 Factor - D 5.1: Adherence to Standards

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
ICT Security Standards	Either no standards or good practices have been identified for use in securing data, technology or infrastructure, by the public and private sectors.Or initial identification of some appropriate standards and good practices has been made by the public and private sectors, and possibly some *ad-hoc* implementation, but no concerted endeavour to implement or change existing practice in a measurable way.	Information risk management standards have been identified for use and there have been some initial signs of promotion and take-up within public and private sectors.There is some evidence of measurable implementation and use of international standards and good practices.	A nationally-agreed baseline of cybersecurity-related standards and good practices have been identified and implemented widely across public and private sectors.An entity within government exists to assess the use of standards across public and private sectors.Government schemes exist to promote continued enhancements, and metrics are being applied to monitor compliance.Consideration is being given as to how standards and best practices can be used to address risk within supply chains within the CI, by both government and CI.	Government and organisations promote use of standards and best practices according to assessment of national risks and budgetary choices.The choice of standards and best practices and their implementation is continuously revised.Emerging cybersecurity risks are regularly assessed and used to re-evaluate the need for additional ICT security standards.There is evidence of debate between government and other stakeholders as to how national and organisational resource decisions should align and drive implementation of standards.Evidence of contribution to international standards' bodies exists and contributes to thought leadership and sharing of experience by organisations.	The country is actively involved in the development and promotion of defined standards internationally.Implementation of standards and non-compliance decisions are made in response to changing threat environments and resource drivers across sectors and CI, through collaborative risk management.Evidence exists of debate within all sectors on compliance to standards and best practices, based on continuous needs assessments.
Standards in Procurement	No standards or best practices have been identified foruse in guiding procurement processes by the public and private sectors. If they are recognised, implementationis *ad hoc* and un-co-ordinated.	Cybersecurity standards and best practices guiding procurement processes(including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services) have been identified for use.Evidence of promotion and implementation ofcybersecurity standards and best practices in defining procurement practices exists within public and private sectors.	Cybersecurity standards and best practices in guidingprocurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services) are being adhered to widely within public and private sectors.Implementation and compliance of standards in procurement practices within the public and private sectors is evidenced through measurement and assessments of process effectiveness.	Organisations have the ability to monitor and change use of standards and best practices in procurement processes, support deviations and non-compliance decisions as the need arises through risk-based decision- making.Emerging cybersecurity risks are regularly assessed and used tore-evaluate the need for additional standards in procurement.Critical aspects of procurement and supply, such as total lifecycle cost, quality, inter-operability,maintenance, support and other value- adding activities, are continuously improved, and procurement process improvements are made in the context of wider resource planning.Organisations are able to benchmark the skills of their procurement professionals against the competencies outlined in procurement standards and identify any skills and capability gaps.	The country is actively involved in the development and promotion of these standards internationally.Implementation of standards in procurement processes and non- compliance decisions are made in response to changing threat environments.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Standards for Provision of Products and Services	Either no standards or best practices have beenidentified for use in securing the products and services (in particular, software, hardware, managed servicesand cloud services) developed or offered by providers in the country.Or there is some identification, but only limited evidence of take-up.	Core activities and methodologies for secure development and lifecycle management for software, hardware and provision of managed services and cloud services are being identified and discussed within professional communities.Government promotes relevant standards in software development, hardware quality assurance, provision of managed services and cloud security but there isno evidence of widespread adoption of these standards yet.	There is evidence of widespread implementation of standardsin the software development processes, hardware quality assurance, provision of managed services and cloud servicesby public and private sector organisations.Government has an established programme for promoting and monitoring standard adoption in software development, hardware quality assurance and cloud security, for public and commercial systems.Evidence that high integrity systems and software development techniques are present within the educational and training offerings in the country.	Security considerations are incorporated in all stages of the development of software, hardware and provision of managed services and cloud services.Core development activities, including configuration and documentation management, security development and lifecycle planning have been adopted into the practices of product and service providersProjects on software development, hardware quality assurance, managed service and cloud security continuously assess the value of standards and reduce or enhance levels of compliance according to risk-based decisions.	The country is actively involved in the development and promotion of these standards internationally.Implementation of these standards and non-compliance decisions are made in response to changing threat environments.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.19 Factor - D 5.2: Security Controls

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Technological Security ontrols	There is minimal or no understanding or deployment of the technological security controls available in themarketplace, by users and public and private sectors.Internet service and other technology providers may not offer any upstream controls to their customers.	Technological security controls are deployed by users and public and private sectors, but possibly not consistently across all sectors.The deployment of up-to-date technological security controls is promoted in an *ad-hoc*manner and all sectors are being incentivised to make use of them.Internet service and other technology providers may be offering security services as part of their services but possibly in an *ad-hoc* manner.Internet service and other technology providers recognise a need to establish internal policies for the deployment of technical security controls, to manage identified risks in the products and services they are offering.	Up-to-date technological security controls, including patching and backups, are deployed in all sectors.Physical security controls are used to prevent unauthorised personnel from entering computing facilities in all sectors.Internet service and other technology providers establish internal policies for the deployment of technical security controls, to manage identified risks in the products and services they are offering.The technological cybersecurity control set reflects internationally-established cybersecurity frameworks, standards and good practice.	Widespread adoption of technological security controls leads to effective upstream protection of users and public and private sectors.All sectors have the capacity to continuously assess the security controls deployed, for their effectiveness and suitability according to their changing needs.The understanding of the technological security controls being deployed extends to their impact on organisationaloperations and budget allocation.The public and private sectors have the capacity to critically assess and upgrade cybersecurity controls according to their appropriateness and suitability for use, and considering emerging risks.There is widespread adoption of multi-factor authentication for online services and privileged accounts. Certificate Authorities are available and digital certificates are widely used.Internet service and other technology providers have the ability to prevent access to non-trusted sites or webaddresses in accordance with the requirements of the appropriate regulator.	The application of advanced technological controls within the country is a leading influence internationally.Implementation of advanced technological security controls are made in response to changing threat environments.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Cryptographic Controls	Cryptographic techniques (e.g.: encryption and digital signatures) for protection of data at rest and data in transit may be a concern but are not yet deployed within the government or private sector, or by the general public.	Cryptographic controls for protecting data at rest and in transit are recognised and deployed *ad hoc* by multiplestakeholders and within various sectors.Tools, such as TLS, are deployed*ad hoc* by service providers to secure all communications between servers and users.	Cryptographic techniques are available for all sectors and users for the protection of data at rest or in transit.There is a broad understanding of secure communication services, such as encrypted or signed email.The cryptographic controls deployed meet international standards and guidelines for each sector and are kept up to date.Tools, such as TLS are routinely deployed by service providers to secure all communications between servers and users.	The public and private sectors critically assess the deployment of cryptographic controls, according to their objectives and priorities.The public and private sectors adapt encryption and cryptographic control policies based on the evolution oftechnological advancement and changing threat environment.The public and private sectors have developed encryption and cryptographic control policies based on the previousassessment, and regularly review the policies for effectiveness.The country has considered implementing digital-identity management.The country has considered whether it requires a national PKI.	The country is contributing to the international debate around best practice on cryptographic controls.Implementation of cryptographic controls are made in response to changing threat environments.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.20 Factor – D 5.3 Software Quality

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Software Quality and Assurance	Quality and performance of software used in the country is a concern, but functional requirements are not yet fully monitored.A catalogue of assured software platforms and applications within the public and private sectors does not exist.Policies and processes regarding updates and maintenance (including patch management) of software applications have not yet been formulated.	Software quality and functional requirements in public and private sectors are recognised and identified, but not necessarily in a strategic manner.A catalogue for assured software platforms and applications within the public and private sectors is in development.Policies and processes on software updates andmaintenance (including patch management) are now in development.Evidence of software quality deficiencies is being gathered and assessed regarding its impact on usability and performance.	Software quality and functional requirements in public and private sectors are recognised and established.Reliable software applications that adhere to international standards and good practices are being used widely in the public and private sectors.Policies on and processes for software updates andmaintenance (including patch management) are established in all sectors.Software applications are characterised as to their reliability, usability and performance in adherence to international standards and good practices.	Quality of software used in public and private sectors is monitored and assessed.Policies and processes on software updates andmaintenance (including patch management) are being improved, based on risk assessments and the critical nature of services in all sectors.Benefits to businesses from additional investment in ensuring software quality and maintenance are measured and assessed.Software defects are manageable in a timely manner and service continuity is ensured.	Software applications of high- level performance, reliability and usability are available, with service continuity processes fully automated.Requirements of software quality are being systematically reviewed, updated, and adapted to the changing cybersecurity environment.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.21 Factor - D 5.4: Communications and Internet Infrastructure Resilience

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Internet Infrastructure Reliability	Affordable and reliable Internet services and infrastructure in the country may not have been established; if they have been, adoption rates of those services are a concern.There is little or no national oversight of network infrastructure.If networks and systems are outsourced, the reliability of third-party providers may not have been considered.Network redundancy measures may be considered, but not in a systematic, comprehensive fashion.	Limited Internet services and infrastructure are available, but with low levels of adoption and issues of unreliability.The ability of Internet infrastructure in public and private sectors to withstand incidents with minimum disruption has been discussed by multiple stakeholders but may not have been fully addressed.Support for securing Internet infrastructure may rely on regional assistance.	Reliable Internet services are widely available and used.Internet services are trusted widely for conductinge-commerce and electronic business transactions; appropriate authentication processes are established.Technology deployed and processes used for managing Internet infrastructure meet international standards and follow good practices.National infrastructure is formally managed, with documented processes, roles and responsibilities, and limited redundancy.	Regular assessments are made of technology, of processes for compliance with international standards, and of guidelines that address the national need inthe face of emerging risks, and changes are made as required.There is effective and controlled acquisition of critical technologies, and there are managed strategic planning and service continuity processes in place.	Acquisition of infrastructure technologies is effectively controlled, with flexibility incorporated according to changing market dynamics.Costs for infrastructure technologies are continually assessed and optimised.Scientific, technical, industrial and human capabilities are being systematically maintained, enhanced, and perpetuated in order to maintain the country's independent resilience.Optimised efficiency is in place to mediate extended outages of systems.
Monitoring and Response	No risk assessments are conducted by Internet infrastructure owners to identify vulnerable assets and prioritise protective actions.There is no monitoring in place to detect that incidents have occurred.No incident response plans are in place.	Processes on developing risk assessments for Internet infrastructure owners have been initiated.There is *ad-hoc* monitoring of parts of the Internetinfrastructure, but it may not be comprehensive.Incident response plans are in development in some sectors.	Mechanisms are in place in both public and private sectors to conduct risk assessments, monitor and test network resilience, and to respond to incidents.Incident response plans are in place in both public and private sectors and are regularly tested and kept under review.Appropriate resources are allocated to hardwareintegration, technology stress testing, personnel training, monitoring, response, and drills to test response plans.	Risks related to emerging and converging technologies are regularly assessed by Internet Infrastructure owners.Risks related to emerging and converging technologies are regularly assessed by regulatory agencies responsible for electronic communications networks and this is used to inform funding and priority decisions.	National-level assets can act to work with the international community in the event of a trans-jurisdictional crisis or incident.Lessons learnt from international collaborations are used toevolve monitoring and response capabilities.Evidence exists that sovereign novel monitoring and response capabilities are being developed in anticipation of emerging threats.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

B.3.22 Factor - D 5.5: Cybersecurity Marketplace

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Cybersecurity Technologies	If domestic production of cybersecurity technologies exists, it does not follow secure processes.The country has not considered the security implications of using foreign cybersecurity technologies.	If there is domestic production, the need for secure processes is recognised.If there is reliance on foreign technologies, the security implications are considered.	If there is domestic production, secure processes are in place.If there is reliance on foreign technologies, the security implications are identified and mitigated in the context of an international supply chain.	If there is local development of cybersecurity technology, it abides by secure codingguidelines, good practices and adheres to internationally- accepted standards.Risk assessments and market incentives inform the prioritisation of productdevelopment and mitigation of identified risks.The security implications of using foreign technologies are routinely analysed and revised based on the assessment of emerging cybersecurity risks.	Security functions in software and computer system configurations are automated in the development and deployment of technologies.Domestic cybersecurity products are exported to other nations and are considered superior products.The country has established a body to assure the security of foreign technologies (devices and software) and supply chains, or to certify entities which can do this.
Cybersecurity Services and Expertise	Cybersecurity consultancy services are not widely on offer in the country.Few if any service providers have professional certification.	There are a growing number of cybersecurity consultancyservices available for private and public organisations.A growing number of service providers provide detail of the professional certifications they possess.There may be limited or no guidance to assist organisations with the selection of service providers.	There are widespread cybersecurity consultancy services available for private and public organisations.All service providers provide details of the professional certifications they possess.A national body accredits service providers, to assist organisations in selecting service providers.	Private and public organisations routinely seek advice from cybersecurity consultancy services, including advice about emerging risks.There is an adequate supply of cybersecurity professionals in the country.	The cybersecurity service sector in the country helps shape the international market.
Security Implications of Outsourcing	No risk assessments are conducted to determine how to mitigate the risks of outsourcing IT to a third party or cloud services.There is a lack of understanding of the security measures that the outsourced IT service provider applies.	Some organisations and sectors conduct risk assessments to determine how to mitigate the risks of outsourcing IT to a third party or cloud services.At least some organisations and sectors understand the security measures that the outsourced IT service provider applies.At least some organisations have developed business continuity and disaster recovery processes.	Most major organisations from the public and private sectors conduct risk assessments to determine how to mitigate the risks of outsourcing IT to a third party or cloud services.There is widespread understanding of the security guarantees provided by the outsourced IT service providers.Most organisations have developed and tested processes to support business continuity and disaster recovery.	Insights arising from risk assessments are routinely analysed in order to establish and promote cybersecurity best practices to mitigate the risk of outsourcing IT.Different risk scenarios with the IT service provider are explored and tested, including emerging risks.	The country is contributing to international best practice on how to mitigate the risk of outsourcing IT.
Cyber Insurance	The need for a cyber-insurance market may have been identified, but no products and servicesare widely available, either domestically or from external providers.	The need for a market in cyber-insurance has been identified through the assessment of financial risks for the public and private sectors, and the appropriateness of availableofferings is now being discussed.	A market for cyber-insurance is established and encourages the sharing of threat-information among participants of the market.Products suitable for small and medium-sized enterprises (SMEs) are also on offer.	Cyber-insurance market offers a variety of covers to mitigate consequential losses.Cover is selected by organisations based on strategic planning needs and identified risk.The cyber-insurance market is innovative and adapts to emerging risks, standards andpractices, while addressing the full scope of cyber harm.Insurance premium reductions are offered for consistent cyber-secure behaviour.	Cyber-insurance practices in the country help to shape the international market.

Aspect	Start-Up	Formative	Established	Strategic	Dynamic
Sharing Vulnerability Information	There is no informal way of sharing information among the stakeholders about the technical details of vulnerabilities.Software and service providers generally lack the ability to address bug and vulnerability reports.	Technical details of vulnerabilities are shared informally with other stakeholders which can distribute the information more broadly.Software and service providers are able to address bug and vulnerability reports but there may not be formal protocols for doing so.	There are formal information- sharing mechanisms or channels in place to share the technical details of vulnerabilities with other stakeholders, which can distribute the information more broadly.A substantial proportion of vulnerabilities in products and services are remedied within defined deadlines after their discovery.	Vulnerability information-sharing mechanisms are continuously reviewed and updated basedon the needs of all affected stakeholders, and in the light of emerging risks.All affected products and services are routinely updated within defined deadline.Processes are in place to review and reduce deadlines where possible.	The country is contributing to the debate and international best practice on the sharing of vulnerability information.
Policies, Processes and Legislation for Responsible Disclosure of Security Flaws	The need for a responsible-disclosure policy in public and private sector organisations, and the right to legal protections for those disclosing security flaws are not yet acknowledged.	The need for a responsible- disclosure policy in public and private sector organisationsis recognised but policies or processes may not be in place, or may only be in development.The right to legal protections for those disclosing security flaws is recognised but legislation may not be in place; or may only be in development.Software and service providers commit to refraining from taking legal action against a party disclosing information responsibly.	A responsible-disclosure policy or framework is in place in public and private sector organisations, and includes a disclosure deadline, scheduled resolution, and the need for acknowledgement.Organisations have established processes to receive and disseminate vulnerability information responsibly.The right to legal protections for those disclosing security flaws responsibly is in place.	Responsible-disclosure policies and processes are continuously reviewed and updated based on the needs of all affected stakeholders and in the light of emerging risks.An analysis of the technical details of vulnerabilitiesis published and advisory information is disseminated according to individual roles and responsibilities.	The country is contributing to the debate on responsible-disclosure frameworks and legal protections for those disclosing security flaws responsibly.

Source: Global Cyber Security Capacity Centre (2021), Cybersecurity Capacity Model for Nations (CMM).

TP-04-22-231-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-604-0
DOI: 10.2824/850466