EUROPEAN UNION AGENCY
FOR CYBERSECURITY

NATIONAL CAPABILITIES ASSESSMENT FRAMEWORK

DECEMBER 2020

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. For more information, visit www.enisa.europa.eu.

CONTACT

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

AUTHORS

Anna Sarri, Pinelopi Kyranoudi – European Union Agency for Cybersecurity (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - 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:

Central State Office for the Development of the Digital Society (Croatia), Marin Ante Pivčević

Centre for Cyber Security (Belgium)

CFCS – Center for Cybersikkerhed (Denmark), Thomas Wulff

European Cybercrime Centre - EC3, Alzofra Martinez Alvaro

European Cybercrime Centre - EC3, Adrian-Ionut Bobeica

Federal Ministry of the Interior (Germany), Sascha-Alexander Lettgen

Information Security Administration (Republic of Slovenia), Marjan Kavčič

Italian Government (Italy)

Malta Information Technology Agency (Malta), Katia Bonello and Martin Camilleri

Ministry of Justice and Public Security (Norway), Robin Bakke

Ministry of Digital Policy (Greece), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali and Sotiris Vasilos

Ministry of Economic Affair and Communication (Estonia), Anna-Liisa Pärnalaas

National Cyber and Information Security Agency (Czech Republic), Veronika Netolická

National Security Authority (Slovakia)

National Security Department (Spain), Maria Mar Lopez Gil

NCTV, Ministry of Justice and Security (Netherlands)

Portuguese National Cybersecurity Centre (Portugal), Alexandre Leite and Pedro Matos

Cyber Security Policy Division, Department of Environment, Climate and Communications (Ireland), James Caffrey

University of Oxford - Global Cyber Security Capacity Centre, Carolin Weisser Harris

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

LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.
This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-443-5

DOI: 10.2824/590072

CATALOGUE: TP-06-20-047-EN-N

1. TABLE OF CONTENTS

GLOSSARY OF TERMS

ACRONYM	DEFINITION
AI	Artificial Intelligence
C2M2	Cybersecurity Capability Maturity Model
CCRA	Common Criteria Recognition Arrangement
CCSMM	The Community Cybersecurity Maturity Model
CII	Critical Information Infrastructure
CMM	Cybersecurity Capacity Maturity Model for Nations
CMMC	Cybersecurity Maturity Model Certification
CPI	Cyber Power Index
CSIRT	Computer Security Incident Response Teams
CVD	Coordinated Vulnerability Disclosure
DPA	Data Protection Act
DSM	Digital Single Market
ECCG	European Cybersecurity Certification Group
ECSM	European Cybersecurity Month
ECSO	European Cyber Security Organisation
EFTA	European Free Trade Association
EQF	European Qualifications Framework
EU	European Union
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulation
GDS	Government Digital Service
IA-CM	Internal Audit Capability Model for the Public Sector
ICT	Information and Communication Technologies
ISMM	Information Security Maturity Model for NIST Cybersecurity Framework
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
MS	Member State
NCSS	National Cybersecurity Strategies

NIS	Network and Information Security
NIST	National Institute of Standards and Technology
NLO	National Liaison Officers
OES	Operators of Essential Services
OT	Operations Technology
PET	Privacy Enhancing Technologies
PIMS	Privacy Information Management System
PPP	Public-private partnerships
Q-C2M2	Qatar Cybersecurity Capability Maturity Model
R&D	Research & Development
SMEs	Small and medium-sized enterprises
SOG-IS MRA	Senior Officers Group for Information Systems' Security, Mutual Recognition Agreement

EXECUTIVE SUMMARY

As the current cyber threat landscape continues to expand and cyber attacks continue to increase in intensity and number, EU Member States need to respond effectively by further developing and adapting their national cybersecurity strategies (NCSS). Since the publication of the first NCSS-related studies by ENISA in 2012, EU Member States and EFTA countries have made great progress in developing and implementing their strategies.

This report presents the work performed by ENISA to build a National Capabilities Assessment Framework (NCAF).

The framework aims at providing Member States with a self-assessment of their level of maturity by assessing their NCSS objectives, that will help them enhance and build cybersecurity capabilities both at strategic and at operational level.

It outlines a simple representative view of the Member State's cybersecurity maturity level. The NCAF is a tool that helps Member States to:

- Provide useful information to develop a long-term strategy (e.g. good practices, guidelines);
- Help identify missing elements within the NCSS;
- Help in further building cybersecurity capabilities;
- Support the accountability of political actions;
- Give credibility towards general public and international partners;
- Support outreach and enhance public image as a transparent organisation;
- Help anticipate the issues lying ahead;
- Help identify lessons learnt and best practices;
- Provide a baseline on cybersecurity capacity across the EU to facilitate discussions; and
- Help evaluate the national capabilities regarding cybersecurity.

This framework was designed with the support of ENISA subject matter experts and representatives from 19 Member States and EFTA countries[1]. The target audience of this report is policymakers, experts and government officials responsible for or involved in designing, implementing and evaluating an NCSS and, on a broader level, cybersecurity capabilities.

[1] Representatives from the following Member States and EFTA countries were interviewed: Belgium, Croatia, Czech Republic, Denmark, Estonia, Germany, Greece, Hungary, Ireland, Italy, Lichtenstein, Malta, Netherlands, Norway, Portugal, Slovakia, Slovenia, Spain, Sweden.

The National Capabilities Assessment Framework covers 17 strategic objectives and is structured around four main clusters:

- Cluster #1: Cybersecurity governance and standards
  1. Develop a national cyber contingency plan
  2. Establish baseline security measures
  3. Secure digital identity and build trust in digital public services

- Cluster #2: Capacity-building and awareness
  4. Organise cyber security exercises
  5. Establish an incident response capability
  6. Raise user awareness
  7. Strengthen training and educational programmes
  8. Foster R&D
  9. Provide incentives for the private sector to invest in security measures
  10. Improve the cybersecurity of the supply chain

- Cluster #3: Legal and regulatory
  11. Protect critical information infrastructure, OES, and DSP
  12. Address cyber crime
  13. Establish incident reporting mechanisms
  14. Reinforce privacy and data protection

- Cluster #4: Cooperation
  15. Establish a public-private partnership
  16. Institutionalise cooperation between public agencies
  17. Engage in international cooperation

1. INTRODUCTION

The Network and Information Security (NIS) Directive, published in July 2016, requires EU Member States to adopt a national strategy on the security of network and information systems, also referred to as an NCSS (National Cyber Security Strategy), as laid down in Articles 1 and 7. In this context, an NCSS is defined as a framework which sets strategic principles, guidelines, strategic objectives, priorities, appropriate policies and regulatory measures. The foreseen objective of an NCSS is to reach and maintain a high level of network and systems security, thus allowing Member States to mitigate potential threats. Moreover, NCSS can also be a catalizer for industrial development and economic and social progress.

The EU Cybersecurity Act states that ENISA shall promote the dissemination of best practices in the definition and implementation of an NCSS by supporting Member States in the adoption of the NIS Directive and by collecting valuable feedback on their experiences. To this end, ENISA has developed several tools to assist the Member States with developing, implementing and evaluating their National Cyber Security Strategies (NCSS).

As part of its mandate, ENISA aims to develop a national capabilities self-assessment framework to measure the level of maturity of the different NCSSs. The objective of this report is to present the study conducted in the definition of the self-assessment framework.

1.1 STUDY SCOPE AND OBJECTIVES

The main objective of this study is to create a national capabilities self-assessment framework, later referred to as NCAF, to measure the level of maturity of the cybersecurity capabilities of the Member States. More specifically, the framework should empower the Member States in:

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

This framework should help the Member States, and in particular national policymakers, to perform a self-assessment exercise with the aim to improve national cybersecurity capabilities.

1.2 METHODOLOGICAL APPROACH

The methodological approach used to develop the national capabilities self-assessment framework relies on four main steps:

1. **Desk Research**: The first step involved conducting an extensive literature review to collect best practices regarding developing a maturity assessment framework for national cybersecurity strategies. The desk research focuses on a systematic analysis of relevant documents on cybersecurity capacity-building and strategy definition, on existing Member States' NCSS's and on a comparison of existing maturity models on cybersecurity. A benchmark exercise on existing maturity models was performed through the adoption of a framework of analysis developed for the purpose of this

study. The framework of analysis builds upon the Becker[2] methodology for the development of maturity models which sets a generic and consolidated procedure model for the design of maturity models and provides clear requirements for the development of maturity models. The framework of analysis was further customised to fulfil the needs of this study.

2. **Collection of experts and stakeholders' point of view**: Based on the data gathered through desk research and the related preliminary findings of the analysis, this phase involved identifying and inviting identified experts that have experience in the development and implementation of an NCSS or of maturity models to interview. ENISA contacted its National Cybersecurity Strategies Experts Group and National Liaison Officers (NLOs) to find the relevant experts in each Member State. Additionally, some experts involved in the development of maturity models were interviewed. Overall, 22 interviews were conducted, 19 of which were conducted with representatives of cybersecurity agencies within different Member States (and EFTA countries).
3. **Analysis of stocktaking input:** The data collected through desk research and the interviews was subsequently analysed to identify best practices in the design of a self-assessment framework to measure the maturity of NCSS's, to understand the needs of the Member States and to determine which data can feasibly be collected in the different European countries[3]. This analysis made it possible to fine-tune the preliminary model developed in the previous steps and to refine the set of indicators included in the model, the maturity levels and its dimensions.
4. **Finalisation of the model:** Thereafter, an updated version of the national capabilities self-assessment framework was reviewed by the ENISA subject matter experts and then further validated by experts through a workshop held in October 2020 prior to publication.

1.3 TARGET AUDIENCE

The target audience of this report is policymakers, experts and government officials responsible for or involved in designing, implementing and evaluating the NCSS and, on a broader level, cybersecurity capabilities. Additionally, the findings formalised in this document can be of value to cybersecurity policy experts and researchers at the national or European level.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, Jun. 2009.

[3] For the purpose of this research, the 'European countries' referenced in this report includes the 27 EU Member States.

2. BACKGROUND

2.1 PREVIOUS WORK ON NCSS LIFECYCLE

As stated in the EU Cybersecurity Act, one of the main goals of ENISA is to support the Member States in developing national strategies on the security of network and information systems, promote the dissemination of those strategies and monitor their implementation. As part of its mandate, ENISA has produced several documents on this subject in order to foster the sharing of good practices and support the implementation of NCSS's across the EU:

- The "Practical guide on the development and execution phase of NCSS"[4] published in 2012
- The "Setting the course for national efforts to strengthen security in cyberspace"[5] published in 2012
- The first ENISA framework for evaluating a Member State's NCSS published[6] in 2014.
- The "Online NCSS Interactive Map"[7] published in 2014.
- The "NCSS Good Practice Guide"[8] published in 2016.
- The "National Cybersecurity Strategies Evaluation Tool"[9] published in 2018.
- The "Good practices in innovation on Cybersecurity under the NCSS"[10] published in 2019.

ANNEX A provides a short summary of ENISA's main publications on this topic.

The abovementioned guides and documents were studied as part of the desk research. In particular, the "National Cybersecurity Strategies Evaluation Tool"[11] is a foundational element of the NCAF. The NCAF builds on the objectives covered in the NCSS online evaluation tool.

2.2 COMMON OBJECTIVES IDENTIFIED WITHIN THE EUROPEAN NCSS

The disparity between the different Member States makes it difficult to identify common activities or action plans among different national contexts, legal frameworks and political

[4] NCSS: Practical Guide on Development and Execution (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] An evaluation framework for NCSS (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, updated in 2019)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] This document updates the 2012 guide: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] National Cybersecurity Strategies Evaluation Tool (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

agendas. However, Member States' NCSS's often have strategic objectives articulated around the same topics. Thus, based on ENISA's previous work and the analysis of Member States' NCSS's, 22 strategic objectives were identified. 15 of these strategic objectives were already identified in ENISA's previous work, 2 were newly added in this study and 5 objectives were identified for future considerations.

2.2.1 Common strategic objectives covered by Member States

Based on ENISA's previous work, namely the National Cybersecurity Strategies Evaluation Tool[12], the following table shows the abovementioned set of 15 strategic objectives that are commonly covered in the Member States' NCSS's. The goals outline the core of the overall 'national philosophy' on the topic. For additional information about the objectives described below, please refer to the ENISA "NCSS Good Practice Guide" report[13].

Table 1: Common strategic objectives covered by Member States in their NCSS

ID	NCSS strategic objectives	Goals
1	**Develop national cyber contingency plans**	▶ Present and explain the criteria that should be used to define a situation as a crisis; ▶ Define key processes and actions for handling the crisis; and ▶ Clearly define the roles and responsibilities of different stakeholders during a cyber-crisis. ▶ Present and explain the criteria for a crisis to be over and/or who has the authority to declare it.
2	**Establish baseline security measures**	▶ Harmonise the different practices followed by the organizations in both the public and the private sector; ▶ Create a common language between the competent public authorities and the organisations and open secure communication channels; ▶ Enable different stakeholders to check and benchmark their cybersecurity capabilities; ▶ Share information about the cybersecurity good practices in every industry sector; and ▶ Help stakeholders to prioritise their investments on security.
3	**Organise cyber security exercises**	▶ Identify what needs to be tested (plans and processes, people, infrastructure, response capabilities, cooperation capabilities, communication, etc.); ▶ Set up a national cyber exercise planning team, with a clear mandate; and ▶ Integrate cyber exercises within the lifecycle of the national cybersecurity strategy or the national cyber contingency plan.
4	**Establish an incident response capability**	▶ Mandate – this relates to the powers, roles and responsibilities that need to be allocated to the team by the respective government; ▶ Service portfolio – this covers the services that a team provides to its constituency or is using for its own internal functioning; ▶ Operational capabilities – this concerns the technical and operational requirements a team must comply with; and ▶ Cooperation capabilities – these encompass requirements regarding information sharing with other teams that are not covered by the previous three categories e.g. policymakers, military, regulators, (critical information infrastructure) operators, law enforcement authorities.

[12] National Cybersecurity Strategies Evaluation Tool (2018) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[13] This document updates the 2012 guide: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide

ID	NCSS strategic objectives	Goals
5	Raise user awareness	▶ Identify gaps in knowledge concerning cybersecurity or information security issues; and ▶ Close the gaps by raising awareness or developing/strengthening knowledge foundations.
6	Strengthen training and educational programmes	▶ Enhance the operational capabilities of the existing information security workforce; ▶ Encourage students to join and then prepare them to enter the cybersecurity field; ▶ Promote and encourage the relations between information security academic environments and the information security industry; and ▶ Align cybersecurity training with business needs.
7	Foster R&D	▶ Identify the real causes of the vulnerabilities instead of repairing their impact; ▶ Bring together scientists from different disciplines to provide solutions to multidimensional and complex problems such as physical-cyber threats; ▶ Bring together the needs of industry and the findings of research, thus facilitating the transition from theory to practice; and ▶ Find ways not only to maintain but also to increase the cybersecurity level of products and services supporting existing cyber infrastructures.
8	Provide incentives for the private sector to invest in security measures	▶ Identify possible incentives for private companies to invest in security measures; and ▶ Provide companies with incentives to encourage security investments.
9	Protect critical information infrastructure, OES, and DSP (CII)	▶ Identify critical information infrastructure; and ▶ Identify and mitigate relevant risks to CII.
10	Address cyber crime	▶ Creating laws in the area of cybercrime; and ▶ Increasing the effectiveness of law enforcement agencies.
11	Establish incident reporting mechanisms	▶ Gain knowledge on the overall threat environment; ▶ Assess the impact of incidents (e.g. security breaches, network failures, service interruptions); ▶ Gain knowledge on existing and new vulnerabilities and types of attacks; ▶ Update security measures accordingly; and ▶ Implement NIS Directive provisions on incident reporting.
12	Reinforce privacy and data protection	▶ Contribute to reinforcing fundamental rights on privacy and data protection.
13	Establish a public-private partnership (PPPs)	▶ Deterring (to deter attackers); ▶ Protecting (uses research into new security threats); ▶ Detecting (uses information sharing to address new threats); ▶ Responding (to deliver the capability to cope with the initial impact of an incident); and ▶ Recovering (to deliver the capability of repairing the final impact of an incident).
14	Institutionalise cooperation between public agencies	▶ Increase the cooperation between public agencies with responsibilities and competencies related to cybersecurity; ▶ Avoid an overlap of competencies and of resources between public agencies; and ▶ Improve and institutionalise cooperation between public agencies in different areas of cybersecurity.
15	Engage in international cooperation (not only with EU MS)	▶ Benefit from creating a common knowledge base between EU Member States; ▶ Create synergy effects between national cybersecurity authorities; and ▶ Enable and increase the fight against transnational crime.

2.2.2 Additional strategic objectives

Based on the desk research performed and the interviews conducted by ENISA, additional strategic objectives were identified. Member States are increasingly addressing these topics in their NCSS or defining action plans on the same subject matter. Examples of activities implemented by Member States are also provided. If an example is from a publicly available source, a reference is provided. In cases where examples are based on confidential interviews with EU Member States' officials, no references are provided.

The following additional strategic objectives were identified:

- Improve the cybersecurity of the supply chain; and
- Secure digital identity and build trust in digital public services.

Improve the cybersecurity of the supply chain

Small and medium-sized enterprises (SMEs) are the backbone of Europe's economy. They represent 99% of all businesses in the EU[14] and in 2015, it was estimated that SMEs have created around 85% of new jobs and provided two thirds of the total private sector employment in the EU. Furthermore, as SMEs provide services to large companies and are increasingly working with public administrations[15], it must be noted that in today's interconnected context, SMEs constitute the weak link for cyber-attacks. Indeed, SMEs are the most exposed to cyber-attacks, yet they often cannot afford to invest adequately in cybersecurity[16]. Improving the cybersecurity of the supply chain should thus be carried out with a focus on SMEs.

In addition to this systemic approach, Member States can also emphasize efforts on the cybersecurity of specific ICT services and products that are considered essential: ICT technologies used in critical information infrastructure, security mechanisms enforced in the telecommunications sector (controls at ISP-level…), trust services as defined in the eIDAS regulation, and cloud service providers. For example, in its 2019-2024 national cybersecurity strategy[17], Poland committed to develop a national cybersecurity assessment and certification system as a mechanism for quality assurance in the supply chain. This certification system will be aligned with the EU certification framework for ICT digital products, services and processes established by the EU Cybersecurity Act (2019/881).

Improving the cybersecurity of the supply chain is thus of paramount importance. This can be achieved by establishing strong policies to promote SMEs, providing guidelines for cybersecurity requirements in public administration procurement procedures, fostering cooperation within the private sector, building PPPs, promoting coordinated vulnerability disclosure (CVD) mechanisms[18], building product certification scheme, including cybersecurity components in digital initiatives for SMEs, and funding skills development, among others.

Secure digital identity and build trust in digital public services

In February 2020, the Commission set out its vision for the digital transformation of the EU in the communication "Shaping Europe's digital future"[19], with the aim of delivering inclusive technologies that work for people and respect the fundamental values of the EU. In particular, the communication states that promoting the digital transformation of public administrations throughout Europe is crucial. In that sense, building trust in government in relation to digital

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16]https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Shaping Europe's digital future, COM(2020) 67 final: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

identity and trust in public services is of paramount importance. This is even more crucial when considering the fact that public sector transactions and data exchanges are often of sensitive nature.

Many countries have expressed their intention to address this topic in their NCSS such as: Denmark, Estonia, France, Luxembourg, Malta, Spain, The Netherlands and The United Kingdom. Among these countries, some have also expressed that this strategic objective might be addressed as part of a broader plan:

- Estonia links their associated action plan on “The security of electronic identity and electronic authentication capability” to the broader Digital Agenda 2020 for Estonia.
- The French NCSS indicates that the Secretary of State responsible for Digital Technology oversees the establishment of a roadmap “to protect the digital lives, privacy and personal data of the French people”.
- The Netherlands NCSS states that cybersecurity in public administrations, as well as public services provided to citizens and businesses are discussed in greater detail in The Broad Agenda for Digital Government.
- As the UK Government continues to move more of its services online, it has appointed the Government Digital Service (GDS) to ensure that all new digital services built or procured by government are also ‘secure by default’, with the support of the British National Cybersecurity Centre (NCSC).

2.2.3 Other strategic objectives considered

During the desk research phase and as part of the interviews conducted by ENISA, other strategic objectives were studied. However, it was decided that these objectives would not form part of the self-assessment framework. ANNEX C – Other objectives studied

provides definitions for each of these objectives that can be used to nurture future discussions on possible NCSS improvements.

The following strategic objectives were studied as future considerations:

- Develop sector-specific cybersecurity strategies.
- Fight against disinformation campaigns.
- Secure cutting-edge technologies (5G, AI, quantum computing…);
- Ensure data sovereignty; and
- Provide incentives for the development of the cyber insurance industry.

2.3 KEY TAKEAWAYS FROM THE BENCHMARK EXERCISE

The desktop research on existing maturity models related to cybersecurity was carried out with the aim of collecting information and evidence to support the design of the national capabilities’ self-assessment framework in the area of NCSS. In this context, an extensive literature review of existing models was conducted to complement the findings from the initial scoping research on cybersecurity maturity models and existing NCSS, developed in sections 2.1 and 2.2. This systematic review supports the selection and justification of the maturity levels of the assessment framework and the definition of the different dimensions and indicators.

In the scope of the systematic review of maturity models, 10 models were considered and analysed on the basis of their key features. The global overview of the key features for each model reviewed in the scope of this study is available in Table 2: Overview of analysed maturity **models** and a more detailed analysis can be found in ANNEX A.

Table 2: Overview of analysed maturity models

Model Name	# of Levels of Maturity	# of Attributes	Assessment Method	Results' Representation
Cybersecurity Capacity Maturity Model for Nations (CMM)	5	5 main dimensions	Collaboration with a local organisation to fine-tune the model before applying it to the national context	5-section radar
Cybersecurity Capability Maturity Model (C2M2)	4	10 main domains	Self-evaluation methodology and toolkit	Scorecard with pie charts
Framework for Improving Critical Infrastructure Cybersecurity	n/a (4 Tiers)	5 core functions	Self-assessment	n/a
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	5	5 main domains	n/a	n/a
Cybersecurity Maturity Model Certification (CMMC)	5	17 main domains	Assessment by third party auditors	n/a
The Community Cybersecurity Maturity Model (CCSMM)	5	6 main dimensions	Assessment within communities with input from state and federal law enforcement agencies	n/a
Information Security Maturity Model for NIST Cybersecurity Framework (ISMM)	5	23 assessed areas	n/a	n/a
Internal Audit Capability Model (IA-CM) for the Public Sector	5	6 elements	Self-assessment	n/a
The Global Cybersecurity Index (GCI)	N/A	5 pillars	Self-assessment	Ranking table
The Cyber Power Index (CPI)	N/A	4 categories	Benchmarking by the Economist Intelligence Unit	Ranking table

This systematic review made it possible to draw conclusions on best practices adopted in existing models in order to support the development of the conceptual model for the current maturity model. In particular, the benchmark exercise supported the definition of the maturity levels, the creation of dimension clusters and the selection of indicators, as well as an appropriate visualisation methodology for the results of the model. The most relevant findings for each of these elements is detailed in Table 3.

Table 3: Key takeaways from the benchmark exercise

Feature	Key takeaway
Levels of Maturity	▶ A five-level maturity scale for assessment frameworks on cybersecurity capabilities is commonly accepted and able to provide granular assessment results (see Table 6 Comparison of Maturity Levels for an exhaustive view of the definition of the levels of maturity for each model); ▶ All models provide a high-level definition of each maturity level that is then adapted to the different dimensions or clusters of dimensions; ▶ Two main aspects are typically assessed when measuring the maturity of cybersecurity capabilities: the maturity of strategies and the maturity of processes put in place to implement strategies.
Attributes	▶ The comparative analysis of the attributes of the existing maturity models shows heterogeneous results with an average number of attributes per model between four and five; ▶ A model relying on around four or five attributes provides countries with the right level of data granularity by grouping relevant dimensions together and ensuring the readability of results (see Table 7: Comparison of Attributes/ **Dimensions** for a description of the attributes for each model); ▶ The key principle adopted by all models when defining the clusters is based in the consistency of element grouped within each cluster.
Assessment method	▶ The assessment methods used in the different models analysed vary from one to another; ▶ The most common assessment method is based on self-evaluation.
Results representation	▶ It is important to present the results at different level of granularity; ▶ The visualisation methodology should be self-explanatory and easy-to-read.

The conceptual model was built based on the benchmarking exercise of the different maturity models as well as on previous work from ENISA. Also, it was decided to build upon the *ENISA online interactive tool* to develop maturity indicators used for each attribute.

2.4 CHALLENGES OF NCSS EVALUATION

Member States are faced with many challenges when building cybersecurity capabilities and more specifically, when ensuring that their capabilities are up to date with the latest developments. Below is a summary of the challenges identified by and discussed with Member States as part of this study:

- **Difficulties in coordination and cooperation:** Coordinating cybersecurity efforts at a national level in order to have an efficient response to cybersecurity issues can prove to be a challenge due to the high number of stakeholders involved.
- **Lack of resources to perform the assessment:** Depending on the local context and cybersecurity national governance structure, evaluating the NCSS and its objectives can take up to more than 15 person-days.
- **Lack of support for developing cybersecurity capabilities:** Some Member States shared that in order to defend a budget and get support to develop cybersecurity capabilities, they first have to carry out an evaluation phase to identify gaps and limitations.
- **Difficulties in attributing successes or changes to the strategy:** As threats evolve every day and technology improves, action plans constantly need to be adapted in response. However, evaluating a NCSS and attributing changes to the strategy itself remains an arduous task. This in turn makes the identification of the limitations and shortcomings of the NCSS difficult.

- **Difficulties to measure the effectiveness of the NCSS:** Metrics can be collected to measure different areas, such as progress, implementation, maturity and effectiveness. While measuring progress and implementation is relatively easy compared to measuring effectiveness, the latter remains more meaningful for evaluating the outcomes and impacts of an NCSS. Based on the interviews conducted by ENISA, a large number of Member States stated that quantitatively measuring the effectiveness of an NCSS is important, but it also represents a very demanding task that is quite impossible in some cases.
- **Difficulty to adopt a common framework:** EU Member States operate in different contexts in terms of politics, organizations, culture, society structure and NCSS maturity. Certain Member States interviewed as part of this study expressed that it might prove difficult to defend and use a “one-size-fits-all” self-assessment framework.

2.5 BENEFITS OF A NATIONAL CAPABILITIES ASSESSMENT

Since 2017, all EU Member States have an NCSS[20]. While a positive development, it is also important that Member States are able to properly assess these NCSS’s, thus bringing added value to their strategic planning and implementation.

One of the goals of the national capabilities assessment framework is to evaluate the cybersecurity capabilities based on the priorities set forth in the various NCSS’s. Fundamentally, the framework assesses the level of maturity of the cybersecurity capabilities of the Member States in the domains defined by the NCSS objectives. Thus, the results of the framework support the Member States’ policymakers in defining the national strategy on cybersecurity by providing them with country intelligence on state of play[21]. The NCAF is ultimately intended to help Member States identify areas of improvement and build capabilities.

The framework aims at providing Member States with a self-assessment of their level of maturity by assessing their NCSS objectives that will help them enhance and build cybersecurity capabilities both at strategic and at operational level.

On a more practical approach, based on the interviews conducted by ENISA with several agencies responsible of the cybersecurity domain in different Member States, the following benefits of the national capabilities assessment framework were identified and underlined:

- Provide useful information to develop a long-term strategy (e.g. good practices, guidelines);
- Help identify missing elements within the NCSS;
- Help in further building cybersecurity capabilities;
- Support the accountability of political actions;
- Give credibility towards general public and international partners;
- Support outreach and enhance public image as a transparent organisation;
- Help anticipate the issues lying ahead;
- Help identify lessons learnt and best practices;
- Provide a baseline on cybersecurity capacity across the EU to facilitate discussions; and
- Help evaluate the national capabilities regarding cybersecurity.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

3. METHODOLOGY OF THE NATIONAL CAPABILITIES ASSESSMENT FRAMEWORK

3.1 GENERAL PURPOSE

The **main objective** of the NCAF is to measure the maturity level of the cybersecurity capabilities of the **Member States** to support them in conducting an evaluation of their national cybersecurity capability, enhancing awareness of the country maturity level, identifying areas for improvement and building cybersecurity capabilities.

3.2 MATURITY LEVELS

The framework is based on **five maturity levels** defining the stages that the Member States go through when building cybersecurity capabilities in the area covered by each NCSS objective. The levels represent increasing levels of maturity, starting from the initial **Level 1**, whereby the Member States do not have a clearly defined approach for cybersecurity capacity-building in the areas covered by the NCSS objectives and finishing with **Level 5**, whereby the cybersecurity capacity-building strategy is dynamic and adaptive to environmental developments. Table 4 shows the maturity level scale with a description of each level of maturity.

Table 4: The ENISA National Capabilities Assessment Framework five-level maturity scale

LEVEL 1 - INITIAL/AD HOC	LEVEL 2 - EARLY DEFINITION	LEVEL 3 - ESTABLISHMENT	LEVEL 4 - OPTIMISATION	LEVEL 5 - ADAPTIVENESS
The Member State does not have a clearly defined approach for cybersecurity capacity-building in the areas covered by the NCSS objectives. Nevertheless, the country might have some generic goals in place and have performed some studies (technical, political, policy) to improve the national capabilities.	The national approach for capacity-building in the area covered by the NCSS objectives has been defined. The action plans or activities to reach the results are in place but at an early stage. Additionally, active stakeholders might have been identified and/or engaged.	The action plan for capacity-building in the area covered by the NCSS objectives is clearly defined and supported by the related stakeholders. The practices and activities are enforced and implemented uniformly at the national level. The activities are defined and documented with clear resource allocation and governance and a set of deadlines.	The action plan is assessed on a regular basis: it is prioritised, optimised and sustainable. The performance of cybersecurity capacity-building activities is regularly measured. Success factors, challenges and gaps in the implementation of activities are identified.	The cybersecurity capacity-building strategy is dynamic and adaptive. Constant attention to environmental developments (technological advancements, global conflict, new threats…) fosters a rapid-decision capability and an ability to act quickly for improvement.

3.3 CLUSTERS & OVERARCHING STRUCTURE OF THE SELF-ASSESSMENT FRAMEWORK

The self-assessment framework is characterised by **four clusters**: (I) Cybersecurity governance and standards, (II) Capacity-building and awareness, (III) Legal and regulatory and (IV) Cooperation. Each of those clusters covers a key thematic area for building cybersecurity capacity in a country and contains a pool of different objectives that the Member States might include in their NCSS. In particular:

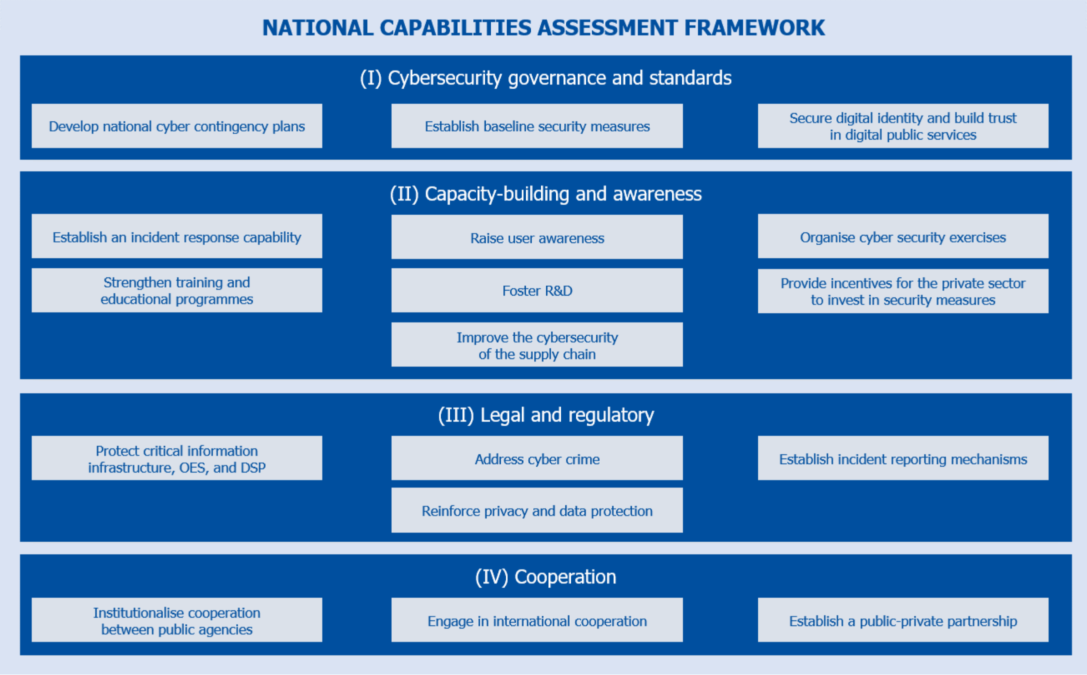
- **(I) Cybersecurity governance and standards**: this cluster measures the capacity of the Member States to establish proper governance, standards and good practices in the cybersecurity domain. This dimension considers different aspects of cyber-defence and resilience while supporting the development of the national cybersecurity industry and building trust in governments;
- **(II) Capacity-building and awareness**: this cluster assesses the capacity of the Member States to raise awareness on cybersecurity risks and threats and on how to tackle them. Additionally, this dimension gauges the ability of the country to continuously build cybersecurity capabilities and increase the overall level of knowledge and skills within this domain. It addresses the development of the cybersecurity market and advancements in cybersecurity R&D**.** This cluster regroups all objectives laying the groundwork to foster capacity-building;
- **(III) Legal and regulatory**: this cluster measures the capacity of the Member States to put in place the necessary legal and regulatory instruments to address and counter the rise of cybercrime and related cyber-incidents, and to protect critical information infrastructure. Additionally, this dimension assess also the capacity of the Member States to create a legal framework to protect citizens and businesses as for instance in the case of balancing security with privacy; and
- **(IV) Cooperation:** this cluster evaluates the cooperation and information sharing between different stakeholder groups at the national and international level as an important tool to better understand and respond to a constantly changing threat environment.

The objectives that have been included in the model are the ones that are commonly adopted by the Member States, and they have been selected among the objectives listed within section 2.2. In particular, the model assesses the following objectives:

- 1. Develop national cyber contingency plans (I)
- 2. Establish baseline security measures (I)
- 3. Secure digital identity and build trust in digital public services (I)
- 4. Establish an incident response capability (II)
- 5. Raise user awareness (II)
- 6. Organise cyber security exercises (II)
- 7. Strengthen training and educational programmes (II)
- 8. Foster R&D (II)
- 9. Provide incentives for the private sector to invest in security measures (II)
- 10. Improve the cybersecurity of the supply chain (II)
- 11. Protect critical information infrastructure, OES, and DSP (III)
- 12. Address cyber crime (III)
- 13. Establish incident reporting mechanisms (III)
- 14. Reinforce privacy and data protection (III)
- 15. Institutionalise cooperation between public agencies (IV)
- 16. Engage in international cooperation (IV)
- 17. Establish a public-private partnership (IV)

The four clusters and underlying objectives are combined in the model to have a holistic view of the maturity of the cybersecurity capabilities of the Member States. Figure 1 presents the overarching structure of the self-assessment framework and shows how these elements, namely, objectives, clusters and self-assessment framework, are linked to evaluating the performance of a country.

Figure 1: Self-assessment framework structure



NATIONAL CAPABILITIES ASSESSMENT FRAMEWORK

(I) Cybersecurity governance and standards

- Develop national cyber contingency plans
- Establish baseline security measures
- Secure digital identity and build trust in digital public services

(II) Capacity-building and awareness

- Establish an incident response capability
- Raise user awareness
- Organise cyber security exercises
- Strengthen training and educational programmes
- Foster R&D
- Provide incentives for the private sector to invest in security measures
- Improve the cybersecurity of the supply chain

(III) Legal and regulatory

- Protect critical information infrastructure, OES, and DSP
- Address cyber crime
- Establish incident reporting mechanisms
- Reinforce privacy and data protection

(IV) Cooperation

- Institutionalise cooperation between public agencies
- Engage in international cooperation
- Establish a public-private partnership

For each objective included within the self-assessment framework, there are a series of indicators distributed between the five levels of maturity. Every indicator is based on a dichotomous (yes/no) question. The indicator can be a requisite or a non requisite.

3.4 SCORING MECHANISM

The **scoring mechanism** of the self-assessment framework takes into consideration the abovementioned elements and the principles listed in section 3.5. In fact, the model provides a score based on the value of two parameters, the **maturity level** and the **coverage ratio**. Each of these parameters can be calculated at different levels: (i) per objective, (ii) per cluster of objectives or (iii) overall.

Scores at objective level

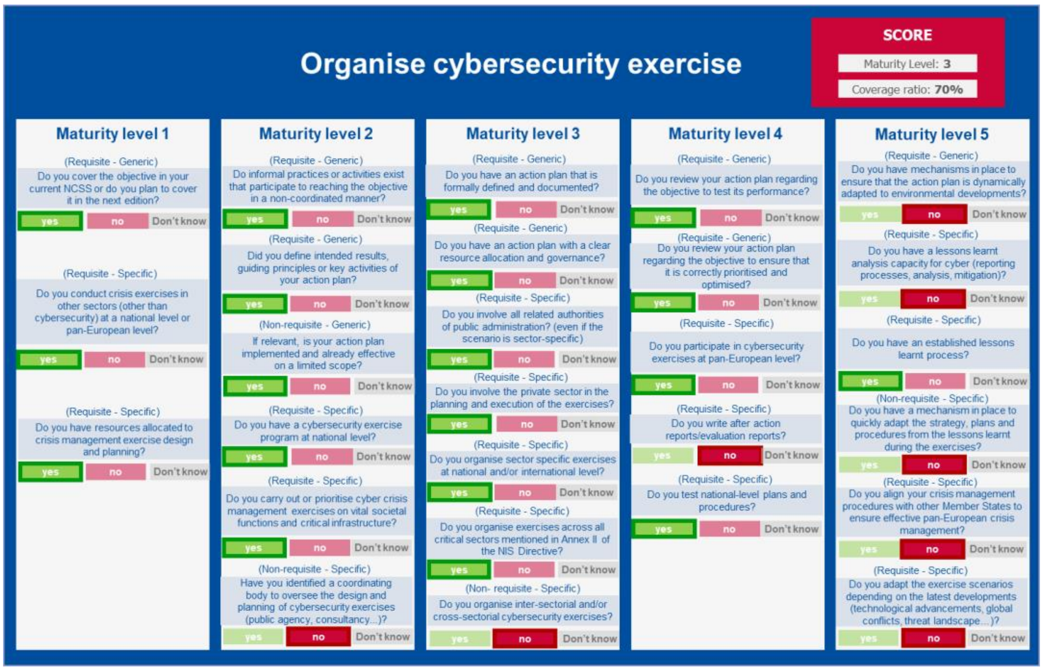
The **maturity level score** gives an overview of the level of maturity by showing what capabilities and practices were put in place. The maturity level score is calculated as the highest level for which the respondent satisfied all the requisites (*i.e.* YES answer to all requisite questions), in addition to having fulfilled all requisites of the previous levels of maturity.

The **coverage ratio** shows the extent of coverage of all the indicators for which the answer is positive, irrespective of their level. It is a complementary value that takes into account all the indicators measuring an objective. The coverage ratio is calculated as the proportion between the total number of questions within the objective and the number of questions for which the answer is positive.

It is important to clarify that for the rest of the document, the word ***score*** is used to refer to both the values of the maturity level and the coverage ratio.

Figure 2 - Scoring mechanism per objective provides a visualisation of the evaluation mechanism described in section 3.1 that will be further developed below.

Figure 2: Scoring mechanism per objective



Organise cybersecurity exercise

SCORE

Maturity Level: **3**

Coverage ratio: **70%**

Maturity level 1

(Requisite - Generic)
Do you cover the objective in your current NCSS or do you plan to cover it in the next edition?
[✓ yes] no Don't know

(Requisite - Specific)
Do you conduct crisis exercises in other sectors (other than cybersecurity) at a national level or pan-European level?
[✓ yes] no Don't know

(Requisite - Specific)
Do you have resources allocated to crisis management exercise design and planning?
[✓ yes] no Don't know

Maturity level 2

(Requisite - Generic)
Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?
[✓ yes] no Don't know

(Requisite - Generic)
Did you define intended results, guiding principles or key activities of your action plan?
[✓ yes] no Don't know

(Non-requisite - Generic)
If relevant, is your action plan implemented and already effective on a limited scope?
[✓ yes] no Don't know

(Requisite - Specific)
Do you have a cybersecurity exercise program at national level?
[✓ yes] no Don't know

(Requisite - Specific)
Do you carry out or prioritise cyber crisis management exercises on vital societal functions and critical infrastructure?
[✓ yes] no Don't know

(Non-requisite - Specific)
Have you identified a coordinating body to oversee the design and planning of cybersecurity exercises (public agency, consultancy...)?
yes [✓ no] Don't know

Maturity level 3

(Requisite - Generic)
Do you have an action plan that is formally defined and documented?
[✓ yes] no Don't know

(Requisite - Generic)
Do you have an action plan with a clear resource allocation and governance?
[✓ yes] no Don't know

(Requisite - Specific)
Do you involve all related authorities of public administration? (even if the scenario is sector-specific)
[✓ yes] no Don't know

(Requisite - Specific)
Do you involve the private sector in the planning and execution of the exercises?
[✓ yes] no Don't know

(Requisite - Specific)
Do you organise sector specific exercises at national and/or international level?
[✓ yes] no Don't know

(Requisite - Specific)
Do you organise exercises across all critical sectors mentioned in Annex II of the NIS Directive?
[✓ yes] no Don't know

(Non- requisite - Specific)
Do you organise inter-sectorial and/or cross-sectorial cybersecurity exercises?
yes [✓ no] Don't know

Maturity level 4

(Requisite - Generic)
Do you review your action plan regarding the objective to test its performance?
[✓ yes] no Don't know

(Requisite - Generic)
Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?
[✓ yes] no Don't know

(Requisite - Specific)
Do you participate in cybersecurity exercises at pan-European level?
[✓ yes] no Don't know

(Requisite - Specific)
Do you write after action reports/evaluation reports?
yes [✓ no] Don't know

(Requisite - Specific)
Do you test national-level plans and procedures?
[✓ yes] no Don't know

Maturity level 5

(Requisite - Generic)
Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?
yes [✓ no] Don't know

(Requisite - Specific)
Do you have a lessons learnt analysis capacity for cyber (reporting processes, analysis, mitigation)?
yes [✓ no] Don't know

(Requisite - Specific)
Do you have an established lessons learnt process?
[✓ yes] no Don't know

(Non-requisite - Specific)
Do you have a mechanism in place to quickly adapt the strategy, plans and procedures from the lessons learnt during the exercises?
yes [✓ no] Don't know

(Requisite - Specific)
Do you align your crisis management procedures with other Member States to ensure effective pan-European crisis management?
yes [✓ no] Don't know

(Requisite - Specific)
Do you adapt the exercise scenarios depending on the latest developments (technological advancements, global conflicts, threat landscape...)?
yes [✓ no] Don't know

Figure 2 shows an example of how the maturity level is calculated by objective. It is worth noting that the respondent fulfilled all the requisites of the first three levels of maturity and only partially fulfilled those of Level 4. Hence, the score indicates that the ***level of maturity of the respondent is Level 3 for the "Organise cybersecurritry exercise" objective****.*

However, in the example depicted in Figure 2, the level of maturity of the objective is not able to capture the information provided by the indicators that have a positive score and that are above Level 3 of maturity. In that case, the coverage ratio can provide an overview of all the elements that the respondent implemented to achieve that objective, despite its actual level of maturity. In this case, the proportion between the total number of questions within the objective and the number of questions for which the answer is positive is equal to 19/27 i.e. ***the coverage ratio value is 70%.***

Additionally, to adapt to the specificities of the Member States whilst also permitting a consistent overview, the score is calculated from two different samples at cluster level and overall level:

- **General scores:** one complete sample covering all the objectives included within the cluster or within the overall framework (from one to 17);
- **Specific scores:** one specific sample covering only the objectives selected by the Member State (usually corresponding to the objectives present in the NCSS of the specific country) within the cluster or within the overall framework.

Scores at cluster level

The **general level of maturity of each cluster** is calculated as the arithmetic mean of the level of maturity of all the objectives within that cluster.

The **specific level of maturity of each cluster** is calculated as the arithmetic mean of the level of maturity of the objectives within that cluster that the Member State chose to assess (usually corresponding to the objectives present in the NCSS of the specific country).

For example, Figure 1 shows that the cluster (I) Cybersecurity governance and standards is composed of three objectives. Assuming that the respondent chose to assess only the first two objectives, but not the third, and assuming that the first two objectives present respectively a level of maturity of 2 and 4, then the level of maturity of the cluster considering all the objectives is Level 2 (Cluster (I) generic maturity level = (2+4)/3), while the level of maturity of the cluster considering only the specific objectives selected by the assessor is Level 3 (Cluster (I) specific maturity level = (2+4)/2).

The **general coverage ratio of each cluster** is calculated as the proportion between the total number of questions within the cluster and the number of questions for which the answer is positive.

The **specific coverage ratio of each cluster** is calculated as the proportion between the total number of questions within the cluster pertaining to objectives that the Member State chose to assess (usually corresponding to the objectives present in the NCSS of the specific country) and the number of questions for which the answer is positive.

Scores at overall level

The **overall general level of maturity of a country** is calculated as the arithmetic mean of the level of maturity of all the objectives within the framework, from one to 17.

The **overall specific level of maturity of a country** is calculated as the arithmetic mean of the level of maturity of the objectives within the framework that the Member State chose to assess (usually corresponding to the objectives present in the NCSS of the specific country)..

The **overall general coverage ratio of a country** is calculated as the proportion between the total number of questions within all the objectives included within the framework (from one to 17) and the number of questions for which the answer is positive.

The **overall specific coverage ratio of a country** is calculated as the proportion between the total number of questions within the objectives within the framework that the Member State chose to assess (usually corresponding to the objectives present in the NCSS of the specific country) and the number of questions for which the answer is positive.

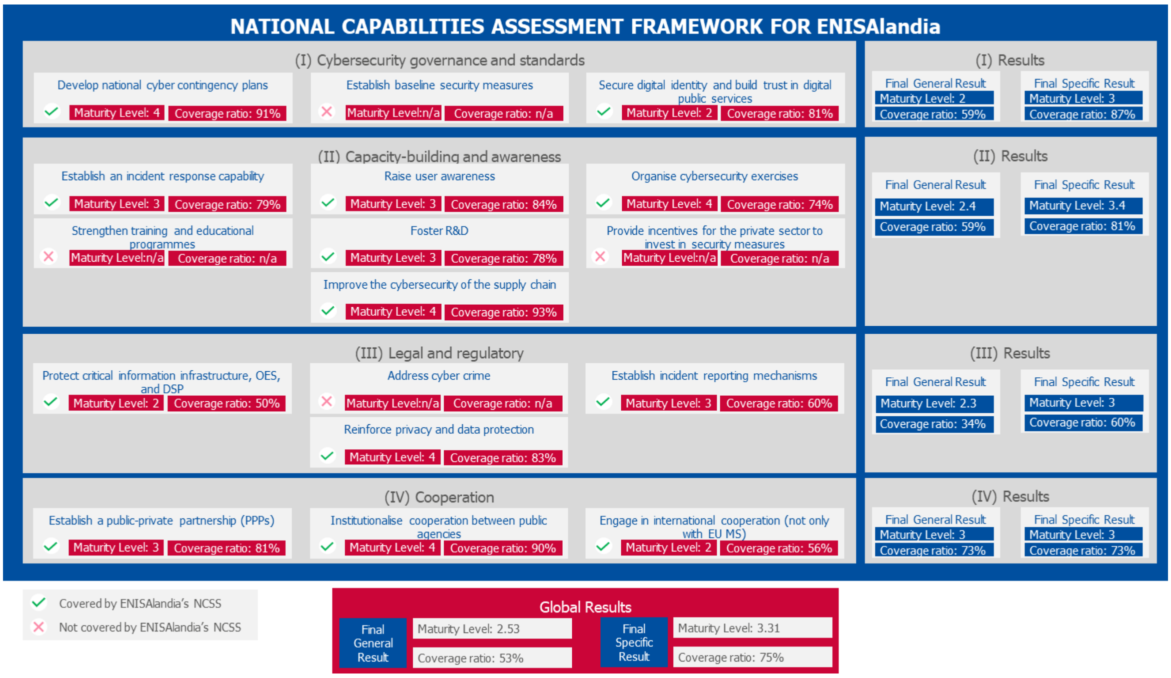
For each indicator, respondents are able to select a third option “don’t know/not applicable” for their response. In this case, the indicator is excluded from the total calculation of the results.

The maturity levels at cluster level and overall level are computed with an arithmetic mean in order to show the progress between two assessments. Indeed, the alternative consisting in computing the cluster and overall maturity levels as the maturity level of the least mature objective – although relevant from a maturity standpoint – cannot account for the progress made in areas covered by other objectives.

Since the cluster level and overall level are consolidated for reporting purposes, the choice has been made to use the arithmetic mean. For more accuracy, please use the scores at objective level for reporting purposes.

Figure 3 below summarizes the scoring mechanisms throughout the different levels of the model (objective, cluster, overall).

Figure 3: Overall scoring mechanism



NATIONAL CAPABILITIES ASSESSMENT FRAMEWORK FOR ENISAlandia

(I) Cybersecurity governance and standards

- ✓ Develop national cyber contingency plans: Maturity Level: 4 | Coverage ratio: 91%
- ✗ Establish baseline security measures: Maturity Level:n/a | Coverage ratio: n/a
- ✓ Secure digital identity and build trust in digital public services: Maturity Level: 2 | Coverage ratio: 81%

(I) Results

	Final General Result	Final Specific Result
Maturity Level	2	3
Coverage ratio	59%	87%

(II) Capacity-building and awareness

- ✓ Establish an incident response capability: Maturity Level: 3 | Coverage ratio: 79%
- ✓ Raise user awareness: Maturity Level: 3 | Coverage ratio: 84%
- ✓ Organise cybersecurity exercises: Maturity Level: 4 | Coverage ratio: 74%
- ✗ Strengthen training and educational programmes: Maturity Level:n/a | Coverage ratio: n/a
- ✓ Foster R&D: Maturity Level: 3 | Coverage ratio: 78%
- ✗ Provide incentives for the private sector to invest in security measures: Maturity Level:n/a | Coverage ratio: n/a
- ✓ Improve the cybersecurity of the supply chain: Maturity Level: 4 | Coverage ratio: 93%

(II) Results

	Final General Result	Final Specific Result
Maturity Level	2.4	3.4
Coverage ratio	59%	81%

(III) Legal and regulatory

- ✓ Protect critical information infrastructure, OES, and DSP: Maturity Level: 2 | Coverage ratio: 50%
- ✗ Address cyber crime: Maturity Level:n/a | Coverage ratio: n/a
- ✓ Establish incident reporting mechanisms: Maturity Level: 3 | Coverage ratio: 60%
- ✓ Reinforce privacy and data protection: Maturity Level: 4 | Coverage ratio: 83%

(III) Results

	Final General Result	Final Specific Result
Maturity Level	2.3	3
Coverage ratio	34%	60%

(IV) Cooperation

- ✓ Establish a public-private partnership (PPPs): Maturity Level: 3 | Coverage ratio: 81%
- ✓ Institutionalise cooperation between public agencies: Maturity Level: 4 | Coverage ratio: 90%
- ✓ Engage in international cooperation (not only with EU MS): Maturity Level: 2 | Coverage ratio: 56%

(IV) Results

	Final General Result	Final Specific Result
Maturity Level	3	3
Coverage ratio	73%	73%

✓ Covered by ENISAlandia's NCSS
✗ Not covered by ENISAlandia's NCSS

Global Results

	Final General Result	Final Specific Result
Maturity Level	2.53	3.31
Coverage ratio	53%	75%

3.5 REQUIREMENTS FOR THE SELF-ASSESSMENT FRAMEWORK

The national capabilities assessment framework presented in this section is based on the needs highlighted by the Member States and it is built around a set of requirements listed hereafter:

- The NCAF is deployed on a voluntary basis by the Member State as a self-assessment framework;
- The NCAF aims at measuring the Member States' cybersecurity capabilities with regards to the 17 objectives. However the Member State can choose the objectives it wants to assess against and only assess a subset of the 17 objectives;
- The self-assessment framework aims at measuring the level of maturity of the cybersecurity capabilities of the Member State;
- The results of the assessment are not published unless the Member State decides to do so on its own initiative;
- The Member State can display the assessment results by presenting the maturity level of the country's cybersecurity capabilities, of a cluster of objectives or even of a single objective;
- All assessed objectives are equally relevant within the assessment framework, therefore, they have the same importance. The same is applicable to the indicators deployed within it; and
- The Member State is able to track its progress over time.

The self-assessment framework aims at supporting the Member States in building cybersecurity capabilities, Hence, it also includes a set of recommendations or guidelines to guide the European countries in improving their level of maturity.

Note: those recommendations or guidelines are generic and based on ENISA publications and lessons learnt from other countries and will depend on the result of the self-assessment.

4. NCAF INDICATORS

4.1 FRAMEWORK INDICATORS

This section presents the ENISA National Capabilities Assessment Framework indicators. The following sections 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. The questionnaire is the main instrument for the self-assessment. For each objective, there are two sets of indicators to be noted:

- A set of generic strategy maturity questions (9 generic questions), marked from ‘a’ to ‘c’ for each maturity level, repeated for each objective; and
- A set of cybersecurity capacity questions (319 cybersecurity capacity questions), numbered from ‘1’ to ‘10’ for each maturity level, specific to the area covered by the objective.

Each question is presented with a tag (0-1) indicating whether the question is a requisite indicator (1) or a non-requisite indicator (0) for the maturity level.

Each question can be identified by an identification number comprised of:

- The objective number;
- The maturity level; and
- The question number.

For example, question ID 1.2.4 is the fourth question in the maturity level 2 of the strategic objective (I) "Develop national cyber contingency plans".

It must be noted that throughout the questionnaire, the scope of the questions is at national level unless otherwise stated. In all questions, the "You" pronoun refers to the Member State in a generic manner and does not refer to the individual or government body carrying out the assessment.

The definition of each objective can be found in chapter 2.2 - Common objectives identified within the European NCSS.

4.1.1 Cluster #1: Cybersecurity governance and standards

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	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…	1	Do you have a doctrine/national strategy that includes cybersecurity as a crisis factor (i.e. a blueprint, a policy, etc.)?	1	Do you have a national-level cyber crisis management plan?	1	Are you satisfied with the number or percentage of critical sectors included in the national cyber contingency plan?	1	Do you have a lessons learning process in place following cyber exercises or actual crises at national level?	1
	2	Is it generally understood that cyber incidents constitute a crisis factor that could threaten national security?	0	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.	1	Do you have national-level cyber crisis-specific procedures?	1	Do you organise activities (i.e. exercises) related to national cyber contingency planning frequently enough?	1	Do you have a process to test the national plan regularly?	1
	3	Have studies (technical, operational, political) been performed on the field of cyber contingency planning?	0	Are the relevant resources engaged to oversee the development and execution of national cyber contingency plans?	1	Do you have a communications team specially trained to respond to cyber crises and inform the public?	1	Do you have sufficient people dedicated to crisis planning, look at the lessons learnt and implement change?	1	Do you have adequate tools and platforms to build situational awareness?	1
	4	-		Do you have a cyber threat assessment methodology at national level that includes procedures for impact assessment?	0	Do you engage all relevant national stakeholders (national security, defense, civil protection, law enforcement, ministries, authorities, etc.?)	1	Do you have sufficient people trained to respond to cyber crises at national level?	1	Do you follow a specific maturity model to monitor and improve the cyber contingency plan?	0
	5	-		-		Do you have adequate crisis management facilities and situation rooms?	1	-		Do you have resources either specialised in threat anticipation or working on prospective cybersecurity to address future crisis or tomorrow's challenges?	0
	6	-		-		Do you engage with international stakeholders in the EU if required?	0	-		-	
	7	-		-		Do you engage with international stakeholders in non-EU countries if required?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	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...	1	Are the security measures drawn in compliance with international/national standards?	1	Are baseline security measures mandatory?	1	Is there a process to frequently update baseline security measures?	1	Do you have a process to harden ICT when incidents fail to be addressed by the measures?	1
	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...	1	Are private sector and other stakeholders consulted when defining baseline security measures?	1	Do you implement horizontal security measures across critical sectors?	1	Is there a monitoring mechanism in place to examine uptake of baseline security measures?	1	Do you evaluate the relevance of new standards that are developed in response to the latest development in the threat landscape?	1
	3	-		-		Do you implement sector specific security measures across critical sectors?	1	Is there a national authority for checking whether baseline security measures are enforced or not?	1	Do you have or promote a national coordinated vulnerability disclosure (CVD) process?	1
	4	-				Are baseline security measures in line with relevant certification schemes?	1	Do you have a process in place to identify non-compliant organisations within a specific period of time?	1	-	
	5	-		-		Is there a self-risk assessment process in place for baseline security measures?	1	Is there an auditing process to ensure that the security measures are applied properly?	1	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2 – Establish baseline security measures	6	-		-		Do you review mandatory baseline security measures in the procurement process of governmental bodies?	0	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…)?	0	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Have you performed studies or gap analyses to identify the needs to secure digital public services to citizens and businesses?	1	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?	1	Do you promote privacy-by-design methodologies in all e-Government projects?	1	Do you collect indicators on cybersecurity incidents involving the breach of digital public services?	1	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…	1
	2	-		Do you have a strategy to build or promote secure national electronic identification schemes (eIDs) for citizens and businesses?	1	Do you include private stakeholders in designing and delivering secure digital public services?	1	Have you implemented mutual recognition of e-identification means with other Member States?	1	Do you actively participate in peer reviews as part of eID schemes notification to the European Commission?	1
	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?	1	Do you implement a minimum security baseline for all digital public services?	1	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	0	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?	1	-		-	
	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?	1	-		-	
	6	-		-		Do you have trust services providers for citizens and businesses (e-signatures, e-seals, e-registered delivery services, time stamping, website authentication)?	1	-		-	
	7	-		-		Do you foster the adoption of baseline security measures for all cloud deployment models (e.g. Private, Public, Hybrid. IaaS, PaaS, SaaS)?	0	-		-	

4.1.2 Cluster #2: Capacity-building and awareness

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Do you have informal incident response capabilities managed within or between public and private sectors?	1	Do you have at least one official national CSIRT ?	1	Do you have incident response capabilities for the sectors referred to in annex II of the NIS Directive?	1	Have you defined and promoted standardised practices for incident response procedures and incident classification schemes?	1	Do you have any mechanisms for early detection, identification, prevention, response and mitigation of zero-day vulnerabilities?	1
	2	-		Does your national CSIRT(s) have a clearly defined scope of intervention? *e.g.* depending on the targeted sector, the types of incident, the impacts	1	Is there a CSIRT cooperation mechanism in your country to respond to incidents?	1	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?	1	-	
	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)?	0	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...	1	-		-	
	4	-				Is there a cooperation mechanism with other neighbouring countries regarding incidents?	1	-		-	
	5	-		-		Have you formally defined clear incident handling policies and procedures?	1	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
4 – Establish an incident response capability	6	-		-		Is your national CSIRT(s) participating in cybersecurity exercises both at national and international level?	1	-		-	
	7	-		-		Is your national CSIRT(s) affiliated with FIRST (Forum of Incident Response and Security Teams)?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	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?	1	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)	1	Have you developed communication plans/strategy for the campaigns?	1	Do you draw up metrics for evaluating your campaign during the planning stage?	1	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?	1
	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.	0	Do you draw up a project plan to raise awareness on information security and privacy issues?	1	Do you have a process for creating content at governmental level?	1	Do you evaluate your campaigns after execution?	1	Do you perform periodic evaluation or study to measure attitude shift or behaviour changes regarding cybersecurity and privacy matters across private and public sectors?	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
5 – Raise user awareness	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.	0	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?	1	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.) ?	1	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…	1	Do you consult with behavioural experts to tailor your campaign towards the target audience?	1
	4	-		-		Do you bring stakeholders with experts and communications teams together to create content?	1			-	
	5	-		-		Do you involve and engage the private sector in your awareness efforts to promote and disseminate the messages to a wider audience?	1	-		-	
	6	-		-		Do you prepare specific awareness initiatives for executives in the public, private, academic or civil society sectors?	1	-		-	
	7	-		-		Do you participate in ENISA European Cybersecurity Month (ECSM) campaigns?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						

6 – Organise cybersecurity exercises	1	Do you conduct crisis exercises in other sectors (other than cybersecurity) at a national level or pan-European level?	1	Do you have a cybersecurity exercise program at national level?	1	Do you involve all related authorities of public administration? (even if the scenario is sector-specific)	1	Do you write after action reports/evaluation reports?	1	Do you have a lessons learnt analysis capacity for cyber (reporting processes, analysis, mitigation)?	1
	2	Do you have resources allocated to crisis management exercise design and planning?	1	Do you carry out or prioritise cyber crisis management exercises on vital societal functions and critical infrastructure?	1	Do you involve the private sector in the planning and execution of the exercises?	1	Do you test national-level plans and procedures?	1	Do you have an established lessons learnt process?	1
	3	-		Have you identified a coordinating body to oversee the design and planning of cybersecurity exercises (public agency, consultancy...)?	0	Do you organise sector specific exercises at national and/or international level?	1	Do you participate in cybersecurity exercises at pan-European level?	1	Do you adapt the exercise scenarios depending on the latest developments (technological advancements, global conflicts, threat landscape...)?	1
	4	-		-		Do you organise exercises across all critical sectors mentioned in Annex II of the NIS Directive?	1	-		Do you align your crisis management procedures with other Member States to ensure effective pan-European crisis management?	1
	5	-		-		Do you organise inter-sectorial and/or cross-sectorial cybersecurity exercises?	1	-		Do you have a mechanism in place to quickly adapt the strategy, plans and procedures from the lessons learnt during the exercises?	0
	6	-		-		Do you organise cybersecurity exercises specific to various levels? (technical and operational level, procedure level, decision-making level, political level...)	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Do you consider developing cybersecurity training and educational programmes?	1	Do you establish courses dedicated to cybersecurity?	1	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?	1	Do you urge personnel in the private and public sector to be accredited or certified?	1	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?	1
	2	-		Do universities of your country offer PhDs in cybersecurity as an independent discipline and not as a computer science subject?	1	Do you have national research labs and educational institutions which are specialized in cybersecurity?	1	Has your country developed cybersecurity training or mentorship programs to support national start-ups and SMEs?	1	Do you establish academic centres of excellence in cybersecurity to act as hubs of research and education?	1
	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.	1	Do you encourage/fund dedicated cybersecurity courses and training plans for employees member-state employment agencies?	1	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.	1	Are academic institutions participating in leading discussions in the area of cybersecurity education and research internationally?	0
	4	-		-		Do you have cybersecurity courses and/or specialised curriculum for EQF (European Qualifications Framework) level 5 to 8?	1	Do you assess the skill gap (cybersecurity workers shortage) in the area of information security on a regular basis?	1	-	
	5	-		-		Do you encourage and/or support initiatives to include internet safety courses in primary and secondary level education?	1	Do you foster networking and information sharing between academic institutions, at both national and international level?	1		

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
7 - Strengthen training and educational programmes	6	-		-		Do you fund or offer for free basic cybersecurity trainings to citizens?	0	Do you involve the private sector in any form in cybersecurity education initiatives? *e.g.* course design and delivery, internships, work placements…	1	-	
	7	-		-		Do you organise annual information security events (e.g. hacking contests or hackathons)?	0	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	0	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Have you performed studies or analyses to identify cybersecurity R&D priorities?	1	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)?	1	Is there a plan to link R&D initiatives with real economy?	1	Are R&D cybersecurity initiatives in line with relevant strategic objectives, e.g. DSM, H2020, Digital Europe, EU cybersecurity strategy?	1	Do you pursue at a national level cooperation with any international R&D initiatives related to cybersecurity?	1
	2	-		Is the private sector involved in setting up R&D priorities?	1	Are there any national projects related to cybersecurity in place?	1	Is there an evaluation scheme in place for R&D initiatives?	1	Are R&D priorities aligned with current or upcoming regulation (national level)?	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
8 – Foster R&D	3	-		Is academia involved in setting up R&D priorities?	1	Do you have local/regional startup ecosystems and other networking channels (e.g. technological parks, innovation clusters, networking events/platforms) to foster innovation (including for cybersecurity startups)?	1	Are there any cooperation agreements with universities and other research facilities?	1	Do you participate in leading discussions in one or many cutting-edge R&D topics at international level?	0
	4	-		Are there any national R&D initiatives related to cybersecurity?	0	Is there investment in cybersecurity R&D programs in academia and the private sector?	1	Is there a recognized institutional body overseeing cybersecurity R&D activities?	0	-	
	5	-		-		Do you have industrial research chairs in universities to bridge research subjects and market needs?	1	-		-	
	6	-		-		Do you have dedicated R&D funding programmes for cybersecurity?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Is there an industrial policy or political will to encourage the development of the cybersecurity industry?	1	Is the private sector involved in the design of incentives?	1	Are there economic/regulatory or other types of incentives in place to promote cybersecurity investments?	1	Are there any private actors that react to incentives by investing in security measures? *e.g.* investors specialised in cybersecurity and non-specialised investors	1	Do you focus incentives on cybersecurity topics depending on the latest threat developments?	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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…	0	Do you provide support (e.g. tax incentives) for cybersecurity startups and SMEs?	1	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…	1	-	
	3	-		-		Do you provide tax incentives or other financial motivation for private sector investors in cybersecurity startups?	1	-		-	
	4	-		-		Do you facilitate access for cybersecurity startups and SMEs in the public procurement process?	0	-		-	
	5	-		-		Is there budget available to provide incentives for the private sector?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	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?	1	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)?	1	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…	1	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)?	1	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…-	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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…	1	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	1	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)?	1	-	
	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?	1	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…	1	-	
	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	0	Do you promote the development of certification schemes targeted at SMEs to boost information security and privacy standard adoption?	0	-	
	5	-		-		Do you provide any types of incentives to SMEs to adopt security and privacy standards?	0	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…	0	-	
	6	-		-		Do you encourage software vendors to support SMEs by ensuring secure default configurations in products targeting small organizations?	0	-		-	

4.1.3 Cluster #3: Legal and regulatory

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Is there a general understanding that CII operators contribute to national security?	1	Do you have a methodology to identify essential services ?	1	Have you implemented the NIS (2016/1148) Directive?	1	Do you have a procedure to update the risk registry?	1	Do you create and update threat landscape reports?	1
	2	-		Do you have a methodology for the identification of CIIs?	1	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?	1	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…	1	Depending on the latest developments in the threat landscape, are you able to onboard a new sector in your CIIP action plan?	1
	3	-		Do you have a methodology to identify OES?	1	Do you have a national registry for identified OES per critical sector?	1	Do you review and consequently update the list of identified OES at least every two years?	1	Depending on the latest developments in the threat landscape, are you able to adapt new requirements in your CIIP action plan?	1

NCSS objective	#										
11 – Protect critical information infrastructure, OES, and DSP	4	-		Do you have a methodology to identify digital service providers?	1	Do you have a national registry for identified digital service providers?	1	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...	1	-	
	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	1	Do you have a national risk registry for identified or known risks?	1	Do you review and consequently update the list of identified digital service providers at least every two years?	1	-	
	6	-		Do you develop sector-specific protection plans? e.g. including baseline cybersecurity measures (mandatory or guidelines)	0	Do you have a methodology to map CII dependencies?	1	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...	1	-	
	7	-		-		Do you deploy risk management practices to identify, quantify and manage risks related to CIIs at a national level?	1	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...	1	-	
	8	-		-		Do you engage in a consultation process to identify cross border dependencies?	1	Do you have mechanisms in place to measure the compliance level of OES and digital service providers with regards to baseline cybersecurity measures?	0	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	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…	0		
	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?	1				
	11	-		-		Do you provide tools or methodologies to detect cyber incidents?	1	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
12 – Address cybercrime	a	Do you cover the objective in your current NCSS, or do you plan to cover it in the next edition?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Have you performed a study to identify the law enforcement requirements (legal basis, resources, skills…) to effectively address cybercrime?	1	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...	1	Do you have units dedicated to handle cybercrime in prosecution offices?	1	Do you collect statistics following the provisions of article 14 (1) of Directive 2013/40/EU (Directive on attacks against information systems) ?	1	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?	1
	2	Have you performed a study to identify the prosecutors and judges requirements (legal basis, resources, skills…) to effectively address cybercrime?	1	Do you have any legal provision addressing online identity theft and personal data theft?	1	Do you have a dedicated budget allocated to cybercrime units?	1	Do you collect separate statistics on cybercrime? e.g. operational statistics, statistics on cybercrime trends, statistics on cybercrime proceeds and induced damage…	1	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…	1
	3	Has your country signed the Council of Europe Budapest Convention on Cybercrime?	1	Do you have any legal provision addressing online intellectual property and copyright infringements?	1	Have you established a central body/entity to coordinate the activities in the area of fighting cybercrime?	1	Do you evaluate the adequacy of the training provided to LEAs, judiciary and national CSIRT(s) personnel to address cybercrime?	1	Is there clear segregation of duties across CSIRTs, LEAs and the judiciary (prosecutors and judges) when they cooperate for adressing cybercrimes?	1
	4			Do you have any legal provision addressing online harassment or cyber-bullying?	1	Have you established cooperation mechanisms between relevant national institutions involved in fighting cybercrime, including law enforcement national CSIRTs?	1	Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to cybercrime units within LEAs?	1	Does your regulatory framework facilitate the cooperation between CSIRTs/LE and judiciary (prosecutors and judges)?	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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	1	Do you cooperate and share information with other Member States in the area of fighting against cybercrime?	1	Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to cybercrime units within prosecution authorities?	1	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…)?	1
	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...	1	Do you cooperate and share information with EU Agencies (e.g. Europol's EC3, Eurojust, ENISA) in the area of fighting against cybercrime?	1	Do you have units dedicated courts or specialized judges to handle cybercrime cases?	1	Do you have any advanced mechanisms in place to deter individuals from being attracted to, or becoming involved in, cybercrime?	0
	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)?	1	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...	1	Do you have any dispositions dedicated to providing support and assistance to victims of cybercrimes (general users, SMEs, large companies)?	1	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?	0
	8			Does your law enforcement agency include a dedicated cybercrime unit?	1	Do you have standard operating procedures to handle e-evidences?	1	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?	1	-	
	9			Have you designated, in accordance with Art. 35. Budapest Convention, a 24/7 point of contact?	1	Does your country participate in training opportunities offered and/or supported by EU Agencies (e.g. Europol, Eurojust, OLAF, Cepol, ENISA)?	0	Does your regulatory framework facilitate the cooperation between CSIRTs and LE?	1	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Is your country considering to adopt the 2nd additional protocol to the Council of Europe Budapest Convention on Cybercrime?	0	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?	1	-	
	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	1						
	12			Has your country ratified/acceded the Council of Europe Budapest Convention on Cybercrime?	1			-	-	-	
	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?	0	-	-	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Do you have informal information sharing mechanisms on cybersecurity incidents incidents between private organisations and national authorities?	1	Do you have an incident reporting scheme for all the sectors under the annex II of the NIS Directive?	1	Do you have a mandatory incident reporting scheme that is functioning in practice?	1	Do you have a harmonised procedure for sectorial incident reporting schemes?	1	Do you create annual incidents report?	1
	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.	1	Is there a coordination/cooperation mechanism for incident reporting obligations regarding GDPR, NISD, article 40 (ex-art13a) and eIDAS?	1	Do you have an incident reporting scheme for sectors others than the ones under the NIS Directive?	1	Are there any cybersecurity landscape reports in place or other kinds of analysis prepared by the entity that receives the incident reports?	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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.	1	Do you have the adequate tools to ensure the confidentiality and integrity of information shared via the various reporting channels?	1	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…	1	-	
	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.	1	Do you have a platform/tool to facilitate the reporting process?	0	Do you have a common taxonomy at national level for incident classification and root cause categories?	0	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Have you performed studies or analyses to identify areas of improvement to better protect the rights of citizen's privacy?	1	Is the national data protection authority involved in cybersecurity related issue areas (e.g. drafting new cybersecurity laws and regulations, defined minimum security measures)?	1	Do you promote best practices on security measures and data protection by design for the public and/or private sector?	1	Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to the data protection authority?	1	Do you have any mechanisms in place to monitor the latest technological developments in order to adapt relevant guidelines and legal provisions/obligations?	1
	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	0	-		Do you launch awareness raising and training programs around this topic?	1	Do you encourage organisations and businesses to get certified against ISO/IEC 27701:2019 on Privacy Information Management System (PIMS)?	1	Do you actively participate/promote R&D initiatives regarding privacy enhancing technologies (PET)?	0
	3	-		-		Do you coordinate incident reporting procedures with the DPA?	1	-		-	
	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)?	0	-		-	
	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?	0	-		-	

4.1.4 Cluster #4: Cooperation

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	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...	1	Do you have a national action plan for establishing PPPs?	1	Have you established national public-private partnerships?	1	Have you established cross-sector PPPs?	1	Depending on the latest technological and regulatory developments, are you able to adapt or create PPPs?	1
	2	-		Do you establish a legal or contractual basis (specific laws, NDAs, intellectual property) to scope PPPs?	1	Have you established sector-specific PPPs?	1	In the established PPPs, do you also focus on public-public and private-private cooperation?	1		
	3	-		-		Do you provide funding for the establishment of PPPs?	1	Do you promote PPPs among small and medium enterprises (SMEs)?	1	-	
	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...	1	Do you measure the outcomes of PPPs?	1	-	
	5	-		-		Are you a member of the European Cyber Security Organisation (ECSO) contractual public-private partnership (cPPP)?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
15 – Establish a public-private partnership (PPPs)	6	-		-		Do you have one or several PPPs working on CSIRT activities?	0	-		-	
	7					Do you have one or several PPPs working on critical information infrastructure protection issues?	0				
	8	-		-		Do you have one or several PPPs working on raising cybersecurity awareness and skills development?	0	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Do you have informal cooperation channels between public agencies?	1	Do you have a national cooperation scheme focused on cybersecurity? *e.g.* advisory boards, steering groups, forums, councils, cyber centres or expert meeting groups	1	Do public authorities participate in the cooperation scheme?	1	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?	1	Are public agencies provided with uniform minimum information on the latest developments of the threat landscape and cybersecurity situational awareness?	1
	2	-		-		Have you established cooperation platforms to exchange information?	1	Do you measure the successes and limits of the different cooperation scheme in fostering effective cooperation?	1	-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
16 – Institutionalise cooperation between public agencies	3	-		-		Have you defined the scope of cooperation platforms (e.g. tasks and responsibilities, number of issue areas)?	1	-		-	
	4	-		-		Do you organise annual meetings?	1	-		-	
	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…	1	-		-	

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do informal practices or activities exist that participate to reaching the objective in a non-coordinated manner?	1	Do you have an action plan that is formally defined and documented?	1	Do you review your action plan regarding the objective to test its performance?	1	Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?	1
	b			Did you define intended results, guiding principles or key activities of your action plan?	1	Do you have an action plan with a clear resource allocation and governance?	1	Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?	1		
	c			If relevant, is your action plan implemented and already effective on a limited scope?	0						
	1	Do you have an international engagement strategy?	1	Do you have cooperation agreements with other countries (bilateral, multilateral) or partners in other countries? *e.g.* information sharing, capacity-building, assistance…	1	Do you exchange information at strategic level? *e.g.* high-level policy, risk perception...	1	Are national cybersecurity public agencies in your country involved in international cooperation schemes?	1	Do you lead discussions on one or many topics within multilateral agreements?	1
	2	Do you have informal cooperation channels with other countries?	1	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…)?	1	Do you exchange information at tactical level? *e.g.* threat actors bulletin, ISACs, TTPs…	1	Do you assess, on a regular basis, the outcomes of international cooperation initiatives?	1	Do you lead discussions on one or many topics within international treaties or conventions?	1

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
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?	1	Do you have dedicated people involved in international cooperation?	1	Do you exchange information at operational level? *e.g.* operational coordination information, ongoing incidents, IOCs…	1	-		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)…	1
	4	-		-		Do you engage in international cybersecurity exercises?	1	-		-	
	5	-		-		Do you engage in international capacity building initiatives? *e.g.* trainings, skills development, drafting standard procedures…	0	-		-	
	6	-		-		Have you established mutual assistance agreements with other countries? *e.g.* LEAs activities, legal proceedings, mutualisation of incident response capabilities, sharing cybersecurity assets…	0	-		-	
	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	0	-		-	

4.2 GUIDELINES TO USE THE FRAMEWORK

This section aims at providing Member States some guidelines and recommendations for rolling out the framework and for filling out the questionnaire. The recommendations listed below are mainly deriving from the feedback collected from the interviews with the Member States' representatives:

- **Anticipate coordination activities to gather data and consolidate data.** Most of the Member States acknowledge that performing such a self-assessment exercise should take around 15 person-days. In order to perform the self-assessment, a large range of different stakeholders will have to be solicited. It is thus recommended to allocate time for the preparation phase to identify all relevant stakeholders within government bodies, public agencies and the private sector.
- **Identify a central body in charge of completing the self-assessment at national level.** As gathering material for all indicators of the NCAF might involve many stakeholders, it is recommended to have a central body or agency tasked with completing the self-assessment by liaising and coordinating with all relevant stakeholders.
- **Use the assessment exercise as a way to share and communicate on cybersecurity topics.** Lessons learnt shared by Member States showed that discussions (whether taking the format of individual interviews or collective workshops) are a good opportunity to foster dialogue around cybersecurity topics and to share common views and areas of improvement. In addition to shining a light on key achievements, sharing results can also help promote cybersecurity topics.
- **Use the NCSS as a scope to select the objectives subjected to the assessment.** The 17 objectives that compose the NCAF were built based on the objectives commonly covered by Member States in their NCSS. The objectives covered as part of the NCSS should be used as a mean to scope the assessment. However, the NCSS should not limit the assessment. As the NCSS naturally focus on priorities, certain areas are purposely omitted from NCSS. However, it does not imply that a given capacity is not present. For example, in the case where a specific objective is omitted from the NCSS, but where the country has cybersecurity capabilities related to that objective, the assessment of that objective can take place.
- **When the NCSS scope evolves, ensure that the score interpretation remains consistent with the NCSS evolution.** The NCSS lifecycle is a multi-year process. Some Member States' NCSS are usually enforced with a 3 to 5-year roadmap with changes in scope between two successive NCSS editions. In that view, special care must be taken when presenting the self-assessment results between two NCSS editions: scope changes might indeed impact the final maturity score. It is recommended to compare the scores on the full scope of strategic objectives from one year to another (*i.e.* Overall general score).

Reminder on the scoring mechanism – example on the coverage ratio

The scoring mechanism includes two levels of scores:

(i) an **overall general coverage ratio** based on the complete list of strategic objectives present in the self-assessment framework; and

(ii) **an overall specific coverage ratio** based on strategic objectives selected by the Member State (usually corresponding to the objectives present in the NCSS of the specific country).

By design (see section 3.1 on the scoring mechanism), the overall specific coverage ratio will be equal or higher than the overall general coverage ratio as the later may include objectives that are not covered by the Member State, thus lowering the overall general coverage ratio. When a Member State adds a new objective, the overall coverage ratio will increase (i.e. more maturity indicators covered), whereas the overall specific maturity may decrease (in case the newly added objective is at a beginning stage and thus has a low level of maturity).

- **When filling out the self-assessment questionnaire, keep in mind that the primary goal is to support Member States in cybersecurity capacity-building.** Therefore, when filling in the self-assessment, even if it can be difficult in some situations to answer the question in a definite manner, it is recommended to choose the answer that is most generally accepted. If, for example, the answer to a question is YES on a certain scope but is NO on another scope, Member States should keep in mind that a NO answer requires an action: either a remediation plan or a plan to act on an improvement area that must be considered in future developments.

5. NEXT STEPS

5.1 FUTURE IMPROVEMENTS

During interviews with Member States' representatives and during the desk research phase, the following recommendations to improve the current National Capabilities Assessment Framework were also identified as potential future evolutions:

- **Develop the scoring system to allow for more accuracy.** For example, a percentage of coverage could be introduced instead of the binary YES/NO answer in order to better account for the complexity of consolidating the capabilities at national level. As a first step, a simple approach with YES/NO answers was chosen.
- **Introduce quantitative metrics to measure the effectiveness of the Member States' NCSS.** Indeed, the National Capabilities Assessment Framework focuses on evaluating the maturity level of the cybersecurity capabilities of the Member States. This could be complemented by metrics to measure the effectiveness of the activities and action plans implemented by the Member States to build these capabilities. It did not seem realistic to build such effectiveness metrics at the current stage given that there is: little feedback from the field, difficulty finding meaningful indicators that link output with NCSS implementation, and difficulty building realistic indicators that can be subsequently gathered. However, this remains a topic for future work.
- **Shift from a self-assessment exercise to an assessment approach.** A potential future evolution of the framework might be the shift towards an assessment approach in order to assess the cybersecurity capabilities maturity of the Member States in a more consistent manner. Having a third party perform the assessment might indeed allow to minimize potential bias.

ANNEX A – DESK RESEARCH RESULTS OVERVIEW

Annex A provides a summary of ENISA previous work on NCSS and a review of relevant publicly available maturity models on cybersecurity capacity. The following assumptions are taken into account for the selection and review of the models:

- Not all models are based on a rigorous research methodology;
- The structure and results of the models are not always explained thoroughly with clear links between the different elements characterising each model;
- Some models do not offer details about the development process, structure and assessment-methodology;
- Other models and tools we found do not offer any details regarding the structure and the content and are therefore not listed; and
- The selection of the models for review is based on geographical coverage. The primary focus will be on maturity models on cybersecurity capacity built to assess the performance of European countries. However, it is important to expand the geographical coverage to analyse good practices in building maturity models around the globe.

This systematic review of relevant publicly available maturity models on cybersecurity capacity was conducted using a customised framework of analysis based on the methodology defined by Becker for the development of maturity models[22]. The following elements were analysed for each existing maturity model:

- **Name of the Maturity Model:** The name of the maturity model and the main references;
- **Institution Source:** The institution, whether public or private, in charge of the design of the model;
- **General Purpose and Target:** The overall scope of the model and the intended target(s);
- **Number and definition of Levels:** The number of maturity levels of the model as well as their general description;
- **Number and name of the Attributes:** The number and name of attributes that the maturity model uses. The attributes' analysis has a three-fold objective:
  - Breakdown the maturity model into easily understandable sections;
  - Aggregate several attributes into clusters of attributes meeting the same goal; and
  - Provide different viewpoints of the maturity level subject.
- **Assessment Method:** The method of assessment of the maturity model;
- **Results' representation**: Define the visualisation method for the results of the maturity model. The logic behind this step is that maturity models tend to fail if they are too complex and therefore, the mode of representation must meet practical needs.

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, Jun. 2009.

Previous work on NCSS

ENISA published two documents on the topic of NCSS's in 2012 as part of its early efforts. Firstly, the "Practical guide on the development and execution phase of NCSS"[23] proposed a set of concrete actions for the efficient implementation of an NCSS and presents the lifecycle of an NCSS in four phases: strategy development, strategy execution, strategy evaluation and strategy maintenance. Secondly, a document called "Setting the course for national efforts to strengthen security in cyberspace"[24] outlined the status of cybersecurity strategies within the EU and beyond in 2012 and proposed that Member States should determine common themes and differences between their NCSS's.

In 2014, the first ENISA framework for evaluating a Member State's NCSS was published[25]. This framework contains recommendations and good practices, as well as a set of capacity-building tools for evaluating an NCSS (*e.g.* identified objectives, inputs, outputs, key performance indicators…). Those tools are adapted to the varying needs of countries at different levels of maturity in their strategic planning. That same year, ENISA published the "Online NCSS Interactive Map"[26], which allows users to quickly consult the NCSS's of all Member States and EFTA countries, including their strategic objectives and good examples of implementation. Developed as first as a NCSS repository (2014), it was updated with examples of implementation in 2018 and since 2019, the map acts now as an *information hub* to centralise data provided by the Member States about their efforts to enhance national cybersecurity.

Published in 2016, the "NCSS Good Practice Guide"[27] identifies fifteen strategic objectives. This guide also analyses the implementation status of each Member State's NCSS and identifies various gaps and challenges with regards to this implementation.

In 2018, ENISA then published the "National Cybersecurity Strategies Evaluation Tool"[28]: an interactive self-assessment tool to help Member States evaluate their strategic priorities and objectives related to their NCSS. Through a set of simple questions, this tool provides Member States with specific recommendations for the implementation of each objective. Finally, the "Good practices in innovation on Cybersecurity under the NCSS"[29] published in 2019 presents the subject of innovation in cybersecurity under the NCSS. The document sets out challenges and good practices across the different innovation dimensions, as perceived by subject-matter experts, in order to help draft future innovative strategic objectives.

A.1 Cybersecurity Capacity Maturity Model for Nations (CMM)

The Cybersecurity Capacity Maturity Model for Nations (CMM) has been developed by the Global Cyber Security Capacity Centre (Capacity Centre), part of the Oxford Martin School within the University of Oxford. The goal of the Capacity Centre is to increase the scale and effectiveness of cybersecurity capacity-building, both within the UK and internationally, through the deployment of the Cybersecurity Capacity Maturity Model (CMM). The CMM is directly targeted at countries that wish to increase their national cybersecurity capacity. Initially

[23] NCSS: Practical Guide on Development and Execution (ENISA, 2012) https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide

[24] NCSS: Setting the course for national efforts to strengthen security in cyberspace (ENISA, 2012) https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

[25] An evaluation framework for NCSS (ENISA, 2014) https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies

[26] National Cybersecurity Strategies - Interactive Map (ENISA, 2014, updated in 2019) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

[27] This document updates the 2012 guide: NCSS Good Practice Guide: Designing and Implementing National Cybersecurity Strategies (ENISA, 2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide

[28] National Cybersecurity Strategies Evaluation Tool (2018) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

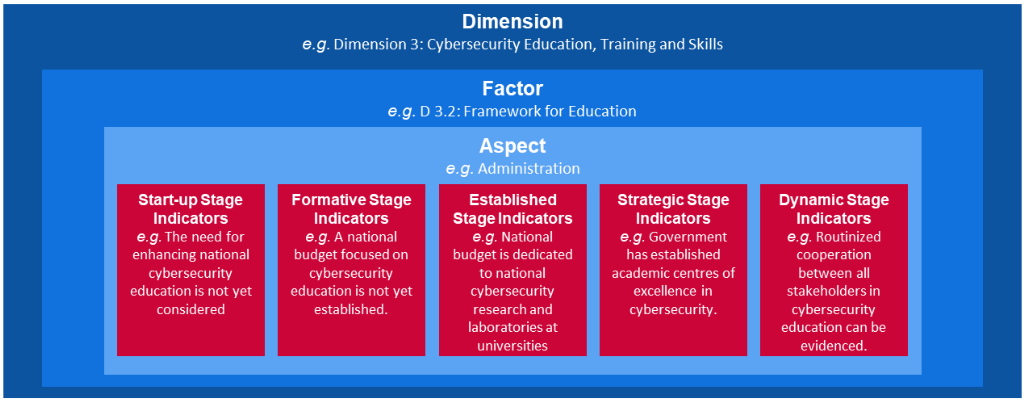
deployed in 2014, the CMM was revised in 2016 following its use in the review of 11 national cybersecurity capacities.

Attributes/ Dimensions

The CMM considers cybersecurity capacity to comprise of **five dimensions** representing the clusters of cybersecurity capacity. Each cluster represents a different research ‘lens’ through which cybersecurity capacity can be studied and understood. Within the five dimensions, **factors** describe the details of possessing cybersecurity capacity. These details are elements that contribute to the enhancement of cybersecurity capacity maturity within each dimension. For each factor, several **aspects** represent different components of the factor. Aspects represent an organisational method to divide indicators into smaller clusters that are easier to comprehend. Each aspect is then evaluated through **indicators** to describe the steps, actions, or building blocks that are indicative of a specific stage of maturity (defined in the next section) within a distinct aspect, factor and dimension.

The terms mentioned above can be layered as shown in the figure below.

Figure 4: Instance of CMM indicators


Dimension
e.g. Dimension 3: Cybersecurity Education, Training and Skills
Factor
e.g. D 3.2: Framework for Education
Aspect
e.g. Administration
Start-up Stage Indicators *e.g.* The need for enhancing national cybersecurity education is not yet considered
Formative Stage Indicators *e.g.* A national budget focused on cybersecurity education is not yet established.
Established Stage Indicators *e.g.* National budget is dedicated to national cybersecurity research and laboratories at universities
Strategic Stage Indicators *e.g.* Government has established academic centres of excellence in cybersecurity.
Dynamic Stage Indicators *e.g.* Routinized cooperation between all stakeholders in cybersecurity education can be evidenced.

The five dimensions are detailed below:

i Devising cybersecurity policy and strategy (6 factors);
ii Encouraging responsible cybersecurity culture within society (5 factors);
iii Developing cybersecurity knowledge (3 factors);
iv Creating effective legal and regulatory frameworks (3 factors); and
v Controlling risks through standards, organisations and technologies (7 factors).

Levels of Maturity

The CMM uses **5 levels of maturity** to determine to which degree a country has progressed in relation to a certain factor/aspect of cybersecurity capacity. These levels serve as a snapshot of the existing cybersecurity capacity:

- **Start-up**: At this stage, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity-building, but no concrete actions have been taken. There is an absence of observable evidence at this stage;
- **Formative**: Some features of the aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply “new”. However, evidence of this activity can be clearly demonstrated;
- **Established**: The elements of the aspect are in place and working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision making has been made concerning the “relative” investment in the various elements of the aspect. However, the aspect is functional and defined;

- **Strategic**: Choices have been made about which parts of the aspect are important, and which are less important for the particular organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional on the nation or organization's particular circumstances; and
- **Dynamic**: At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technology of the threat environment, global conflict or a significant change in one area of concern (*e.g.* cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

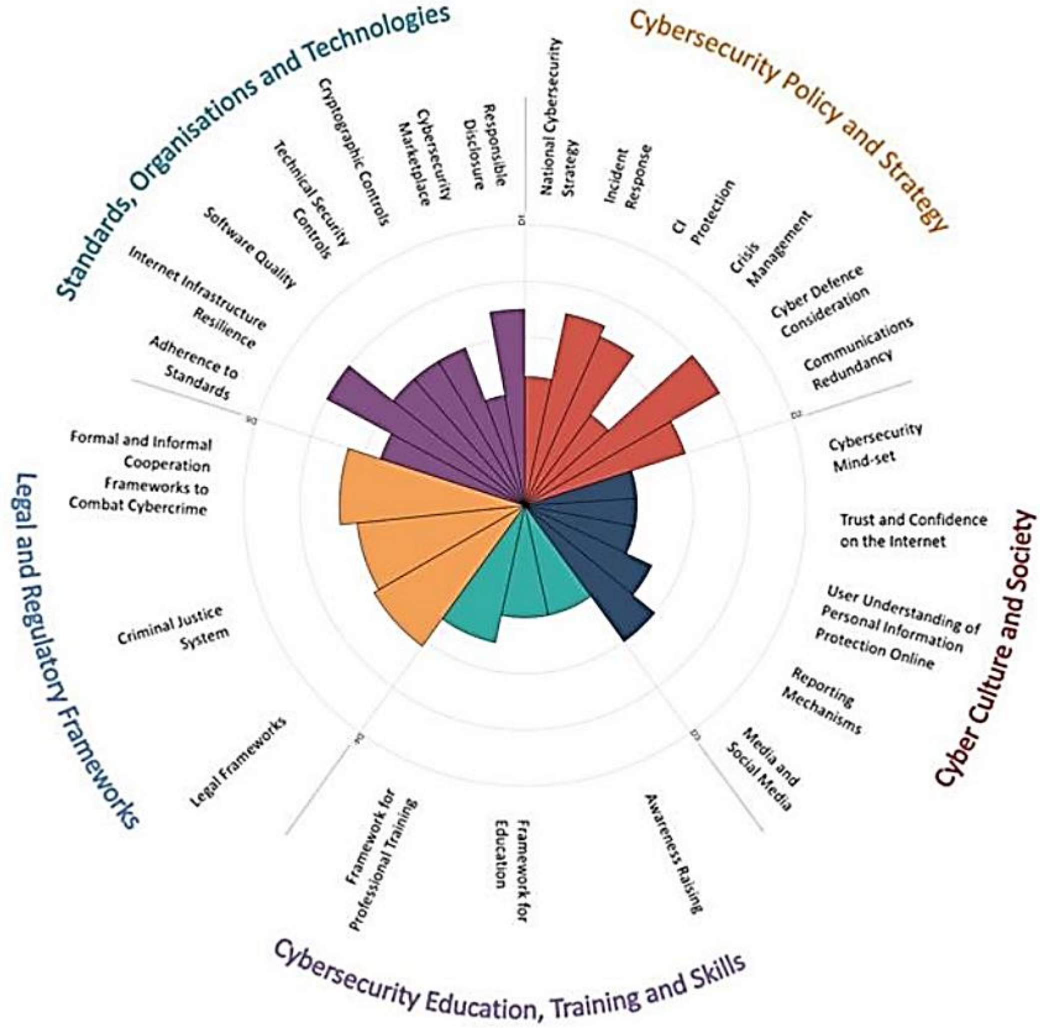
Assessment Method

As the Capacity Centre does not have a thorough and in-depth understanding of each domestic context in which the model is deployed, it works alongside international organisations, host ministries or organisations within the respective country to review the cybersecurity capacity maturity. In order to assess the level of maturity of the five dimensions included in the CMM, the Capacity Centre and the host organisation meets with relevant national stakeholders of the public and private sectors over the course of 2 or 3 days to conduct focus groups on the dimensions of the CMM. Each dimension is discussed at least twice by different clusters of stakeholders. This constitutes the preliminary pool of data for the subsequent assessment.

Mode or representation of the results

The CCM provides an overview of the maturity level of each country through a radar composed of five sections, one for each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; as shown below, ‘start-up’ is closest to the centre of the graphic and ‘dynamic’ is at the perimeter.

Figure 5 CMM: Results overview



Global Cyber Security Capacity Centre Oxford Martin School, University of Oxford, 2017.

A.2 Cybersecurity Capability Maturity Model (C2M2)

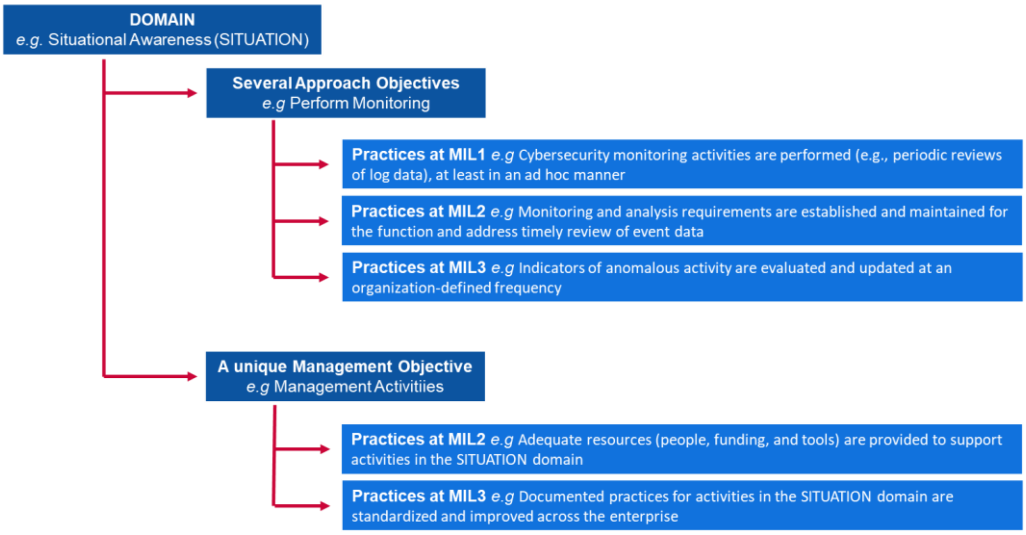
The Cybersecurity Capacity Maturity Model (C2M2) has been developed by the U.S. Department of Energy in collaboration with private and public sector experts. The goal of the Capacity Centre is to help organizations of all sectors, types, and sizes to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience. The C2M2 focuses on the implementation and management of cybersecurity practices associated with information, information technology (IT), and operations technology (OT) assets and the environments in which they operate. The C2M2 defines maturity models as: “a set of characteristics, attributes, indicators, or patterns that represent capability and progression in a particular discipline”. Initially deployed in 2014, the C2M2 was revised in 2019.

Attributes/ Dimensions

The C2M2 considers **ten domains** representing a logical grouping of cybersecurity practices. Each set of practices represents the activities an organization can perform to establish and mature capability in the domain. Each domain is then associated with a **unique management objective** and **several approach objectives**. Within both approach and management objectives, **several practices** are detailed to describe institutionalized activities.

The relationship between these notions is summed up below:

Figure 6: Instance of C2M2 indicator


DOMAIN
e.g. Situational Awareness (SITUATION)
Several Approach Objectives
e.g Perform Monitoring
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner
Practices at MIL2 e.g Monitoring and analysis requirements are established and maintained for the function and address timely review of event data
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency
A unique Management Objective
e.g Management Activitiies
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the enterprise

The ten domains are detailed below:

i Risk Management (RISK);
ii Asset, Change, and Configuration Management (ASSET);
iii Identity and Access Management (ACCESS);
iv Threat and Vulnerability Management (THREAT);
v Situational Awareness (SITUATION);
vi Event and Incident Response (RESPONSE);
vii Supply Chain and External Dependencies Management (DEPENDENCIES);
viii Workforce Management (WORKFORCE);
ix Cybersecurity Architecture (ARCHITECTURE); and
x Cybersecurity Program Management (PROGRAM).

Levels of Maturity

The C2M2 uses **4 levels of maturity** (named Maturity Indicator Levels – MIL) to determine a dual progression of maturity: an approach progression and a management progression. The MILs range from MIL0 to MIL3 and are meant to be applied independently to each domain.

- **MIL0**: Practices are not performed.
- **MIL1**: Initial practices are performed but may be ad hoc.
- **MIL2**: Management characteristics:
  - Practices are documented;
  - Adequate resources are provided to support the process;
  - Personnel performing the practices have adequate skills and knowledge; and
  - Responsibility and authority for performing the practices are assigned.

  Approach characteristic:
  - Practices are more complete or advanced than at MIL1.
- **MIL3**: Management characteristics:
  - Activities are guided by policies (or other organizational directives);
  - Performance objectives for domain activities are established and monitored to track achievement; and
  - Documented practices for domain activities are standardized and improved across the enterprise.

  Approach characteristic:
  - Practices are more complete or advanced than at MIL2.

Assessment Method

The C2M2 is designed for use with a **self-evaluation methodology** and toolkit (available by request) for an organization to measure and improve its cybersecurity program. A self-evaluation using the toolkit can be completed in one day, but the toolkit could be adapted for a more rigorous evaluation effort. Additionally, the C2M2 can be used to guide the development of a new cybersecurity program.

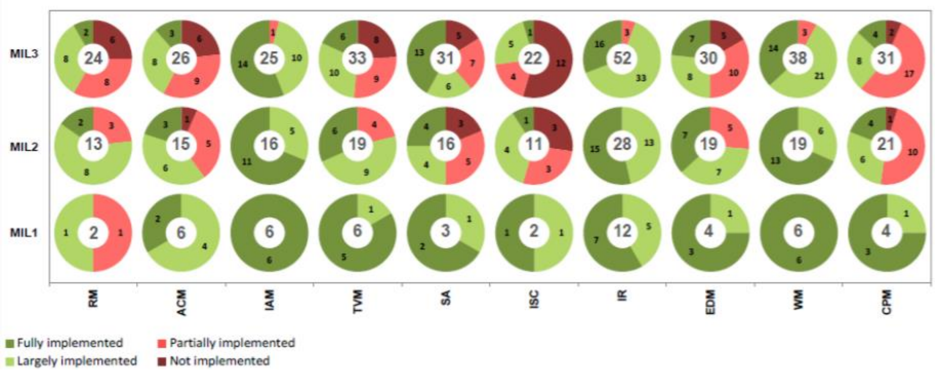
The model content is presented at a high level of abstraction so it can be interpreted by organizations of various types, structures, sizes, and industries. Broad use of the model by a sector can support benchmarking of the sector's cybersecurity capabilities.

Mode or representation of the results

The C2M2 provides an Evaluation Scoring Report generated from the survey results. The report presents results in two views: the Objective view, which shows practice question responses by each domain and its objectives, and the Domain view, which shows responses by all domains and MILs. Both views are based on a representation system characterised by pie charts (or "doughnuts"), one per response, and a traffic light system scoring mechanism. As shows in Figure 7, the red sectors in a doughnut chart show a count of the number of questions that received survey responses of "Not Implemented" (dark red) or "Partially Implemented" (light red). The green sectors show the number of questions that received responses of "Largely Implemented" (light green) or "Fully Implemented" (dark green).

Figure 7 below is an example of a scoring card at the end of a maturity assessment. In the X axis are the 10 domains of the C2M2, and in the Y axis, the levels of maturity (MILs). Looking at the graph and considering the domain of Risk Management (RM), it is possible to notice three pie charts, one corresponding to each level of maturity MIL1, MIL2 and MIL3. For the domain RM, the graph highlights that there are two items to be evaluated for reaching the first level of maturity, MIL1. In this case, one scoring "largely implemented" and one scoring "Partially implemented". For the second level on maturity, MIL2, the model foresees 13 items to be evaluated. Two of those 13 items belong to the first level, MIL1, and 11 to the second level, MIL2. The same is applicable for the third level MIL3.

Figure 7: C2M2 – Domain view example



Source: U.S. Department of Energy, Office of electricity delivery and energy reliability, 2015.

A.3 Framework for Improving Critical Infrastructure Cybersecurity

The Framework for Improving Critical Infrastructure Cybersecurity was developed within the National Institute of Standards and Technology (NIST). It focuses on guiding cybersecurity activities and managing risks within an organisation. It is aimed at all types of organisations regardless of size, degree of cybersecurity risk, or cybersecurity sophistication. As this is a framework and not a model, it is built differently than the models analysed previously.

The Framework consists of three parts: the Framework Core, the Implementation Tiers, and the Framework Profiles:

- The **Framework Core** is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors. These are similar to the attributes or dimensions found in cybersecurity capacity maturity models.
- **Framework Implementation Tiers** ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. Tiers do not represent maturity levels, rather, they are meant to support organizational decision making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and could receive additional resources.
- A **Framework Profile** ("Profile") represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized with regards to the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario. Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a "Current" profile (the "as is" state) with a "Target" profile (the "to be" state).

Framework Core

The Framework Core consists of five **Functions**. When considered together, these Functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk. The Framework Core then identifies underlying key **Categories** and **Subcategories** for each Function and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

Functions and Categories are detailed below:

i **Identify**: Develop an organizational understanding about how to manage cybersecurity risks for systems, people, assets, data, and capabilities.
  - Subcategories: Asset Management; Business Environment; Governance; Risk Assessment; and Risk Management Strategy

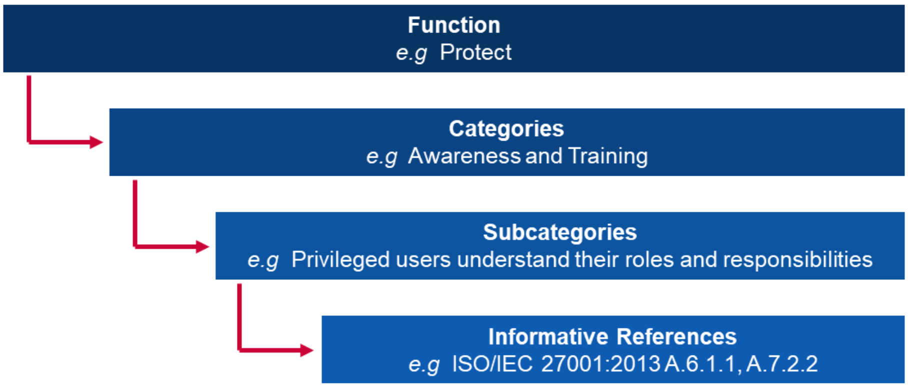
ii **Protect**: Develop and implement appropriate safeguards to ensure delivery of critical services.
  - Subcategories: Identity Management and Access Control; Awareness and Training; Data Security; Information Protection Processes and Procedures; Maintenance; and Protective Technology

iii **Detect**: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
  - Subcategories: Anomalies and Events; Security Continuous Monitoring; and Detection Processes.

iv **Respond**: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
  - Subcategories: Response Planning; Communications; Analysis; Mitigation; and Improvements.

v **Recover**: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
  - Subcategories: Recovery Planning; Improvements; and Communications

Figure 8: Instance of the Framework for Improving Critical Infrastructure Cybersecurity


Function
e.g Protect
Categories
e.g Awareness and Training
Subcategories
e.g Privileged users understand their roles and responsibilities
Informative References
e.g ISO/IEC 27001:2013 A.6.1.1, A.7.2.2

Tiers

The Framework for Improving Critical Infrastructure Cybersecurity relies on **4 Tiers**, each of which is defined along three axes: Risk Management Process, Integrated Risk Management Program and External Participation. The Tiers are not to be considered as maturity levels but as a framework to provide organizations with a contextualisation of their views of cybersecurity risk and the processes in place to manage that risk.

- **Tier 1: Partial**
  - **Risk Management Process**: organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner;
  - **Integrated Risk Management Program**: there is limited awareness of cybersecurity risk at the organizational level. The organization implements cybersecurity risk management on an irregular, case-by-case basis and may not have processes that enable cybersecurity information to be shared within the organization;
  - **External Participation**: the organization does not understand its role in the larger ecosystem with respect to either its dependencies or dependents. The organization is generally unaware of the cyber supply chain risks of the products and services it provides and that it uses;
- **Tier 2: Risk Informed**
  - **Risk Management Process**: risk management practices are approved by management but may not be established as organizational-wide policy;
  - **Integrated Risk Management Program**: there is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established. Cyber risk assessment of organizational and external assets occurs but is not typically repeatable or reoccurring;
  - **External Participation**: generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. Additionally, the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses but does not act consistently or formally upon those risks;
- **Tier 3: Repeatable**
  - **Risk Management Process**: the organization's risk management practices are formally approved and expressed as policy. Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape;
  - **Integrated Risk Management Program**: there is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures

are defined, implemented as intended, and reviewed. Senior executives ensure consideration of cybersecurity through all lines of operation in the organization;
  - External Participation: the organization understands its role, dependencies, and dependents in the larger ecosystem and may contribute to the community's broader understanding of risks. The organization is aware of the cyber supply chain risks associated with the products and services it provides and that it uses;

- **Tier 4: Adaptive**
  - **Risk Management Process**: the organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators;
  - **Integrated Risk Management Program**: there is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events; and
  - External Participation: the organization understands its role, dependencies, and dependents in the larger ecosystem and contributes to the community's broader understanding of risks.

Assessment Method

The Framework for Improving Critical Infrastructure Cybersecurity is meant for organisations to self-assess their risk in order to make their cybersecurity approach and investments more rational, effective and valuable. To examine the effectiveness of investments, an organization must first have a clear understanding of its organizational objectives, the relationship between those objectives and supportive cybersecurity outcomes. The cybersecurity outcomes of the Framework Core support self-assessment of investment effectiveness and cybersecurity activities.

A.4 Qatar Cybersecurity Capability Maturity Model (Q-C2M2)

The Qatar Cybersecurity Capability Maturity Model (Q-C2M2) was developed by the Qatar University's College of Law in 2018. The Q-C2M2 is based on various existing models to build a comprehensive assessment methodology to enhance Qatar's cybersecurity framework.

Attributes/ Dimensions

The Q-C2M2 adopts the National Institute of Standards and Technology (NIST) Framework's approach of using five core functions as the main domains of the model. The five core functions are applicable in the Qatari context because they are common across critical infrastructure sectors, an important element in the Qatari cybersecurity framework. The Q-C2M2 is based on **five domains**, each domain is then divided in several **subdomains** to cover the whole range of cybersecurity capability maturity.

The five domains are detailed below:

i. The **Understand domain** includes four subdomains: Cyber governance, Assets, Risks, and Training;
ii. Subdomains under the **Secure domain** include Data Security, Technology Security, Access Control Security, Communications Security, and Personnel Security;
iii. The **Expose domain** includes the subdomains of Monitoring, Incident Management, Detection, Analysis, and Exposure;
iv. The **Respond domain** includes Response Planning, Mitigation, and Response Communication; and
v. The **Sustain domain** includes Recovery Planning, Continuity Management, Improvement, and External Dependencies.

Levels of Maturity

The Q-C2M2 uses **5 levels of maturity** measuring the capability maturity of a state entity or non-state organization at the core function level. These levels are aimed at assessing maturity in the five domains detailed in the previous section.

- **Initiating**: Employs ad-hoc cybersecurity practices and processes under some of the domains;
- **Implementing**: Adopted policies to implement all of the cybersecurity activities under the domains with the aim of completing the implementation at a certain time;
- **Developing**: Implemented policies and practices to develop and improve cybersecurity activities under the domains with the aim of suggesting new activities to implement;
- **Adaptive**: Revisits and reviews cybersecurity activities and adopts practices based on predictive indicators derived from previous experiences and measures; and
- **Agile**: Continues to practice the adaptive stage with an added emphasis on agility and speed when implementing activities in the domains.

Assessment Method

The Q-C2M2 is at an early stage of research and is not yet built for implementation. It is a framework that could be used to deploy a detailed assessment model for Qatari organisations in the future.

A.5 Cybersecurity Maturity Model Certification (CMMC)

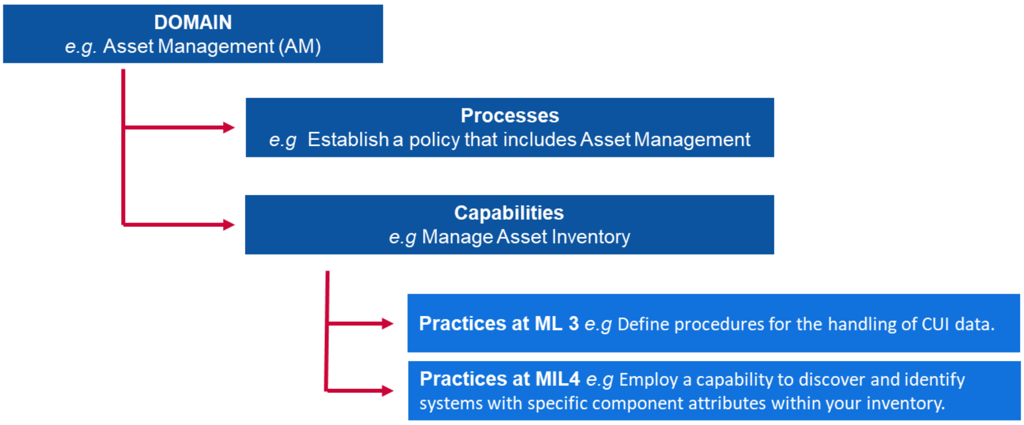
The Cybersecurity Maturity Model Certification (CMMC) was developed by the U.S. Department of Defense (DoD) in collaboration with Carnegie Mellon University and Johns Hopkins University Applied Physics Laboratory. The main objective of the DoD in the design of this model is to protect information from the Defense Industrial Base sector (DIB). The information targeted by the CMMC is classified as either “Federal Contract Information”, information provided by or generated for the Government under contract not intended for public release, or “Controlled Unclassified Information”, information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations and government-wide policies. The CMMC measures cybersecurity maturity and provides best practices along with a certification element to ensure the implementation of practices associated with each maturity level. The latest version of the CMMC was released in 2020.

Attributes/ Dimensions

The CMMC considers **seventeen domains** representing clusters of cybersecurity processes and capabilities. Each domain is then broken down into multiple **processes** that are similar across domains; and one to many **capabilities** spanning over five levels of maturity. The capabilities (or capability) are then detailed into **practices** for each relevant maturity level.

The relationship between these notions is as follows:

Figure 9: Instance of CMMC indicators



DOMAIN
e.g. Asset Management (AM)
Processes
e.g Establish a policy that includes Asset Management
Capabilities
e.g Manage Asset Inventory
Practices at ML 3 *e.g* Define procedures for the handling of CUI data.
Practices at MIL4 *e.g* Employ a capability to discover and identify systems with specific component attributes within your inventory.

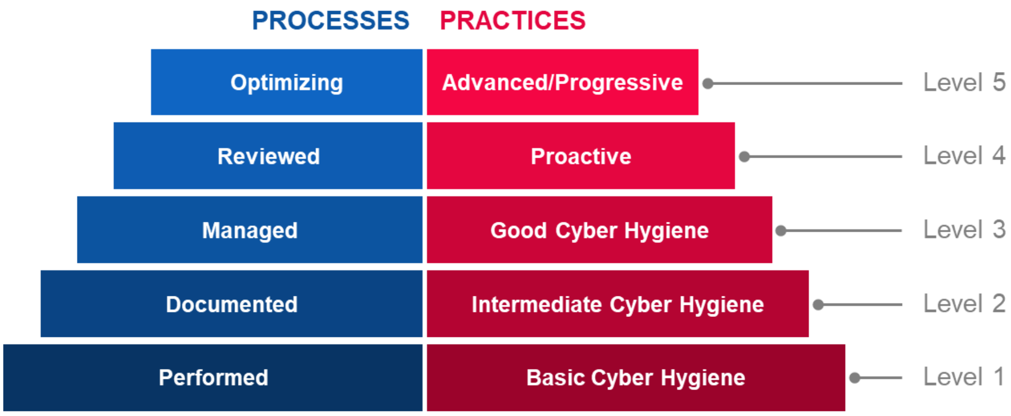
The seventeen domains are detailed below:

i Access Control (AC);
ii Asset Management (AM);
iii Audit and Accountability (AU);
iv Awareness and Training (AT);
v Configuration Management (CM);
vi Identification and Authentication (IA);
vii Incident Response (IR);
viii Maintenance (MA);
ix Media Protection (MP);
x Personnel Security (PS);
xi Physical Protection (PE);
xii Recovery (RE);
xiii Risk Management (RM);
xiv Security Assessment (CA);
xv Situational Awareness (SA);
xvi System and Communications Protection (SC); and
xvii System and Information Integrity (SI).

Levels of Maturity

The CMMC uses **5 levels of maturity** defined based on processes and practices. In order to reach a certain level of maturity in the CMMC, an organization needs to fulfil the prerequisites for the processes and the practices for that level itself. This also implies the fulfillment of the prerequisites of all the level below that one.

Figure 10: CMMC Maturity Levels



- **Level 1**
  - **Processes – Performed**: because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation. Process maturity is not assessed for Level 1;
  - **Practices – Basic Cyber Hygiene**: level 1 focuses on the protection of FCI (Federal Contract Information) and consists only of practices that correspond to the basic safeguarding requirements;
- **Level 2**
  - **Processes – Documented**: level 2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented;
  - **Practices – Intermediate Cyber Hygiene**: level 2 serves as a progression from Level 1 to Level 3 and consists of a subset of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references;

- **Level 3**
  - **Processes – Managed**: level 3 requires that an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders;
  - **Practices – Good Cyber Hygiene**: level 3 focuses on the protection of CUI and encompasses all of the security requirements specified in NIST SP 800-171 as well as additional practices from other standards and references to mitigate threats;
- **Level 4**
  - **Processes – Reviewed**: level 4 requires that an organization review and measure practices for effectiveness. In addition to measuring practices for effectiveness, organizations at this level are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis;
  - **Practices – Proactive**: level 4 focuses on the protection of CUI (Controlled Unclassified Information) and encompasses a subset of the enhanced security requirements. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques, and procedures;
- **Level 5**
  - **Processes – Optimizing**: level 5 requires an organization to standardize and optimize process implementation across the organization; and
  - **Practices – Advanced/Proactive**: level 5 focuses on the protection of CUI. The additional practices increase the depth and sophistication of cybersecurity capabilities.

Assessment Method

The CMMC is a relatively young model, finalised in the first quarter of 2020. Thus far, it has not been deployed within any organisations. Nevertheless, the DoD contractors expect to reach out to certified third party examiners to conduct audits. The DoD is expecting its contractors to implement best practices to foster cybersecurity and the protection of sensitive information.

A.6 The Community Cyber Security Maturity Model (CCSMM)

The Community Cyber Security Maturity Model (CCSMM) was developed by the Centre for Infrastructure Assurance and Security within The University of Texas. The goal of the CCSMM is to better define methods to determine the current status of a community in its cyber-preparedness and provide a roadmap for communities to follow in their preparation efforts. The communities targeted by the CCSMM are mainly local or state governments. The CCSMM was designed in 2007.

Attributes/ Dimensions

Levels of maturity are defined following **6 main dimensions** that cover the different aspects of cybersecurity within communities and organisations. These dimensions are clearly defined for each level of maturity (detailed in the Figure 31: Summary of the **CCSMM**) The 6 dimensions are:

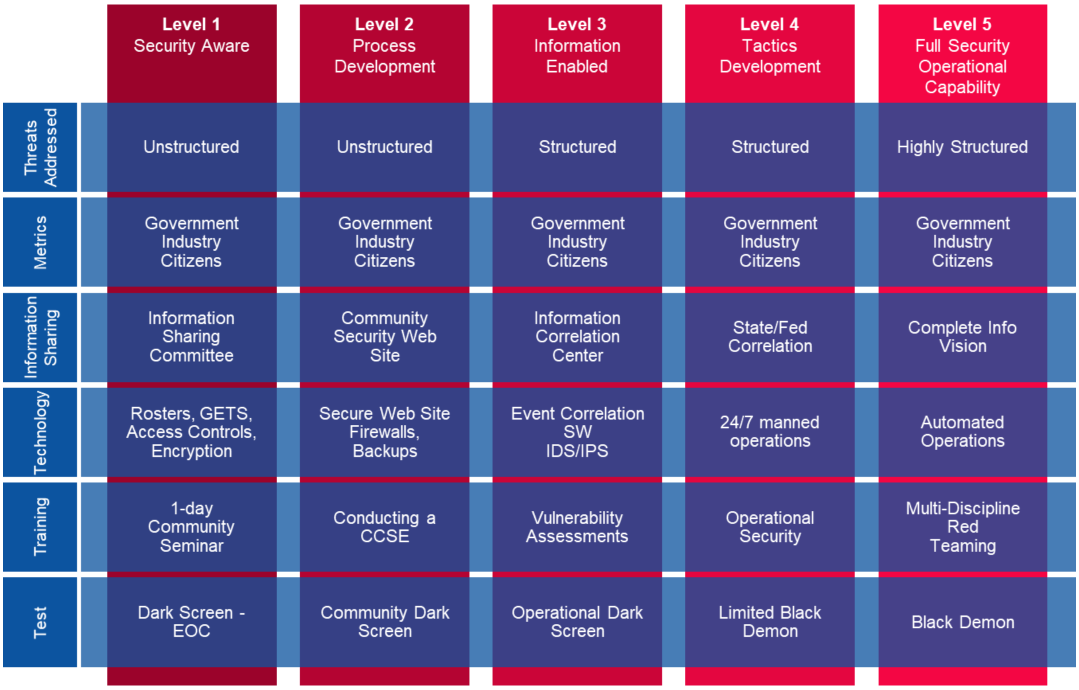
i Threats Addressed;
ii Metrics;
iii Information Sharing;
iv Technology;
v Training; and
vi Test.

Levels of Maturity

The CCSMM relies on **5 levels of maturity** based on the main types of threats and activities addressed at the level:

- **Level 1: Security Aware**
  The major theme of activities at this level is to make individuals and organizations aware of the threats, problems, and issues related to cybersecurity;
- **Level 2: Process Development**
  Level designed to help communities establish and improve security processes required to effectively address cybersecurity issues;
- **Level 3: Information Enabled**
  Designed to improve information sharing mechanisms within the community to enable the community to effectively correlate seemingly disparate pieces of information.
- **Level 4: Tactics Development**
  This level elements are designed to develop better and more proactive methods to detect and respond to attacks. By this level, most prevention methods should be in place.
- **Level 5: Full Security Operational Capability**
  This level represents those elements that should be in place for any organization to consider itself fully operationally ready to address any type of cyber threat.

Figure 31: Summary of the CCSMM dimensions per level



	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Assessment Method

The CCSMM as an assessment methodology is meant to be deployed by communities with input from state and federal law enforcement agencies. It aims to help the community to define what is most important, what are the most likely targets, and what needs to be protected (and to which extent). With these objectives in mind, plans can be developed to bring each aspect of the community to their required level of cybersecurity maturity. The specific intelligence generated by the CCSMM helps to define the goals of various tests and exercises that can be used to measure the effectiveness of established programs.

A.7 Information Security Maturity Model for NIST Cyber Security Framework (ISMM)

The Information Security Maturity Model (ISMM) has been developed within the College of Computer Sciences and Engineering of the King Fahd University of Petroleum and Minerals in Saudi Arabia. It proposes a new capability maturity model to measure the implementation of cybersecurity measures. The goal of the ISMM is to enable organisations to measure their implementation progress over time by using the same measuring tool on a regular basis to ensure that the desired security posture is maintained. The ISMM was developed in 2017.

Attributes/ Dimensions

The ISMM builds on the existing assessed areas of the NIST framework and adds a dimension on compliance assessment. This brings the model to **23 assessed areas** to for an organisation’s security posture. The 23 assessed areas are:

i Asset Management;
ii Business Environment;
iii Governance;
iv Risk Assessment;
v Risk Management Strategy;
vi Compliance Assessment;
vii Access Control;
viii Awareness and Training;
ix Data Security;
x Information Protection Processes and Procedures;
xi Maintenance;
xii Protective Technology;
xiii Anomalies and Events;
xiv Security Continuous Monitoring;
xv Detection Processes;
xvi Response Planning;
xvii Response Communications;
xviii Response Analysis;
xix Response Mitigation;
xx Response Improvements;
xxi Recovery Planning;
xxii Recovery Improvements; and
xxiii Recovery Communications.

Levels of Maturity

The ISMM relies on **5 levels of maturity**, which, unfortunately are not detailed in the available documentation.

- **Level 1:** Performed Process;
- **Level 2:** Managed Process;
- **Level 3:** Established Process;
- **Level 4:** Predictable Process; and
- **Level 5:** Optimizing Process.

Assessment Method

The ISMM does not propose any specific methodology to conduct the assessment for organisations.

A.8 Internal Audit Capability Model (IA-CM) for the Public Sector

The Internal Audit Capability Model (IA-CM) was developed by the Institute of Internal auditors Research Foundation with the intention to build capacity and advocacy through self-assessment in the public sector. Aimed at audit professionals, the IA-CM provides an overview of the model itself along with an Application Guide to assist in the use of the model as a self-assessment tool.

Despite the IA-CM being focused on Internal Audit capability, rather than cybersecurity capacity-building, the model is built as a maturity self-assessment tool for public sector entities that can be applied globally to improve processes and effectiveness. As the scope is not focused on cybersecurity, the attributes will not be analysed. The IA-CM was finalised in 2009.

Levels of Maturity

The Internal Audit Capability Model (IA-CM) includes **5 levels of maturity**, each of which describe the characteristics and capabilities of an Internal Audit activity at that level. The capability levels in the model provide a road map for continuous improvement.

- **Level 1: Initial**
  No sustainable, repeatable capabilities – dependent upon individual efforts
  - Ad hoc or unstructured.
  - Isolated single audits or reviews of documents and transactions for accuracy and compliance.
  - Outputs dependent upon the skills of the specific person holding the position.
  - No professional practices established other than those provided by professional associations.
  - Funding approval by management, as needed.
  - Absence of infrastructure.
  - Auditors likely part of a larger organizational unit.
  - Institutional capability is not developed.
- **Level 2: Infrastructure**
  Sustainable and repeatable practices and procedures
  - Key question or challenge for Level 2 is how to establish and maintain repeatability of processes and thus a repeatable capability.
  - internal audit reporting relationships, management and administrative infrastructures, and professional practices and processes are being established (internal audit guidance, processes, and procedures).
  - Audit planning based principally on management priorities.
  - Continued reliance essentially on the skills and competencies of specific persons.
  - Partial conformance with the standards.
- **Level 3: Integrated**
  Management and professional practices uniformly applied
  - Internal audit policies, processes, and procedures are defined, documented, and integrated into each other and the organization’s infrastructure.
  - Internal audit management and professional practices are well established and uniformly applied across the internal audit activity.
  - Internal audit is starting to align with the organization’s business and the risks it faces.
  - internal audit evolves from conducting only traditional internal audit to integrating as a team player and providing advice on performance and management of risks.
  - Focus is on team building and capacity of the internal audit activity and its independence and objectivity.
  - Generally conforms with the standards.
- **Level 4: Managed**
  Integrates information from across the organization to improve governance and risk management
  - Internal audit and key stakeholders’ expectations are in alignment.
  - Performance metrics are in place to measure and monitor internal audit processes and results.
  - Internal audit is recognized as delivering significant contributions to the organization.

- Internal audit functions as an integral part of the organization’s governance and risk management.
- Internal audit is a well-managed business unit.
- Risks are measured and managed quantitatively.
- Requisite skills and competencies are in place with a capacity for renewal and knowledge sharing (within internal audit and across the organization).

Level 5: Optimizing

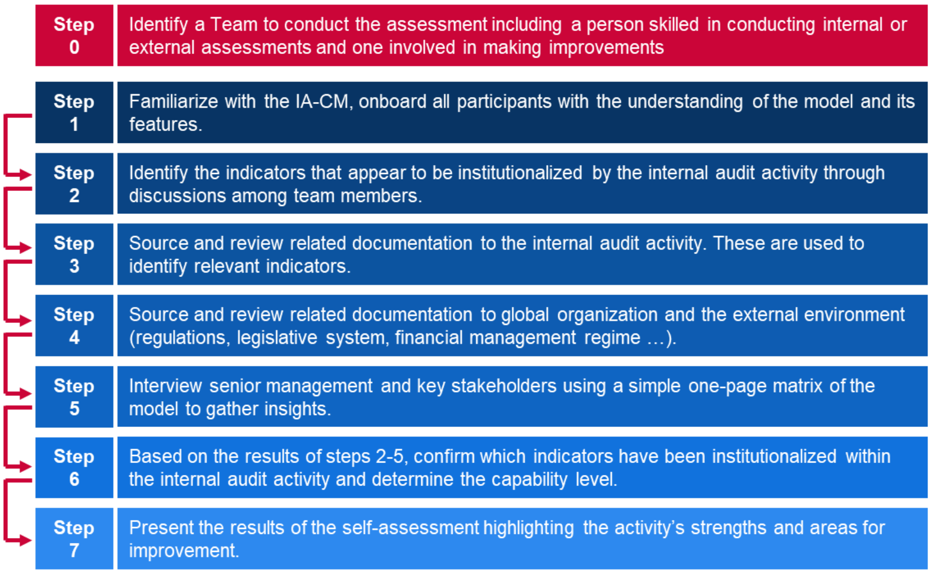
Learning from inside and outside the organization for continuous improvement

- Internal audit is a learning organization with continuous process improvements and innovation.
- Internal audit uses information from inside and outside the organization to contribute to achieving strategic objectives.
- World-class/recommended/best practice performance.
- Internal audit is a critical part of the organization’s governance structure.
- Top-level professional and specialized skills.
- Individual, unit, and organizational performance measures are fully integrated to
- drive performance improvements.

Assessment Method

The Internal Audit Capability Model is clearly built for self-assessment. It provides detailed steps to follow for using the IA-CM and a sample slides deck to customize. Prior to the start of the self-assessment, a specific team is to be identified, including, at minimum, one person skilled in conducting internal or external assessments of internal audits and one person who is involved in making improvements in this area.

Figure 12: IC-AM Self-Assessment Steps



Step 0 Identify a Team to conduct the assessment including a person skilled in conducting internal or external assessments and one involved in making improvements

Step 1 Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.

Step 2 Identify the indicators that appear to be institutionalized by the internal audit activity through discussions among team members.

Step 3 Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.

Step 4 Source and review related documentation to global organization and the external environment (regulations, legislative system, financial management regime …).

Step 5 Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.

Step 6 Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capability level.

Step 7 Present the results of the self-assessment highlighting the activity’s strengths and areas for improvement.

A.9 The Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI) is an initiative of the International Telecommunication Union (ITU) aimed at reviewing the cybersecurity commitment and situation in all the ITU regions: Africa, Americas, Arab States, Asia-Pacific, CIS, and Europe, and puts countries with high commitment and recommendable practices in the spotlight. The goal of the GCI is to help countries identify areas for improvement in the field of cybersecurity, as well as motivate them to take action to improve their ranking, thus helping raise the overall level of cybersecurity worldwide.

As the GCI is an index and not a maturity model, it doesn’t use levels of maturity but rather a score to rank and compare the global cybersecurity commitment of nations and regions.

Attributes/ Dimensions

The Global Cybersecurity Index (GCI) is based on the five pillars of the Global Cybersecurity Agenda (GCA). These pillars form the five sub-indices of the GCI and each includes a set of indicators. The five pillars and indicators are as follows:

i **Legal**: measures based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.
  - Cybercrime legislation;
  - Cybersecurity regulation; and
  - Containment/curbing of spam legislation.

ii **Technical**: Measures based on the existence of technical institutions and frameworks dealing with cybersecurity.
  - CERT/CIRT/CSRIT;
  - Standards Implementation Framework;
  - Standardization Body;
  - Technical mechanisms and capabilities deployed to address Spam;
  - Use of cloud for cybersecurity purposes; and
  - Child Online Protection mechanisms.

iii **Organizational**: Measures based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.
  - National Cybersecurity Strategy;
  - Responsible Agency; and
  - Cybersecurity.

iv **Capacity-building**: Measures based on the existence of research and development, education and training programmes, certified professionals and public sector agencies fostering capacity-building.
  - Public awareness campaigns;
  - Framework for the certification and accreditation of cybersecurity professionals;
  - Professional training courses in cybersecurity;
  - Educational programs or academic curricular in cybersecurity;
  - Cybersecurity R&D programs; and
  - Incentive mechanisms.

v **Cooperation**: Measures based on the existence of partnerships, cooperative frameworks and information sharing networks.
  - Bilateral agreements;
  - Multilateral agreements;
  - Participation in international fora/associations;
  - Public-Private Partnerships;
  - Inter-agency/intra-agency partnerships; and
  - Best Practices.

Assessment Method

The GCI is a self-assessment tool built through a survey[30] of binary, pre-coded, and open-ended questions. The use of binary answers eliminates opinion-based evaluation and any possible bias towards certain types of answers. The pre-coded answers save time and allow a more accurate data analysis. Moreover, a simple dichotomous scale allows for a quicker and more complex evaluation as it does not require lengthy answers, which accelerates and streamlines the process of providing answers and further evaluation. The respondent should only confirm presence of, or lack of, certain pre-identified cybersecurity solutions. An online survey mechanism, which is used for gathering answers and uploading relevant material, enables the extraction of good practices and a set of thematic qualitative evaluations by a panel of experts.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

The overall GCI process is implemented as follows:

- A letter of invitation is sent to all participants, informing them of the initiative and requesting a focal point responsible for collecting all relevant data and for completing the online GCI questionnaire. During the online survey, the approved focal point is officially invited by ITU to answer the questionnaire;
- Primary data collection (for countries that do not respond to the questionnaire):
  - ITU elaborates an initial draft response to the questionnaire using publicly available data and online research;
  - The draft questionnaire is sent to focal points for review;
  - Focal points improve the accuracy and then return the draft questionnaire;
  - The corrected draft questionnaire is sent to each focal point for final approval; and
  - The validated questionnaire is used for analysis, scoring, and ranking.
- Secondary data collection (for countries that respond to the questionnaire):
  - ITU identifies any missing responses, supporting documents, links, etc;
  - The focal point improves the accuracy of the responses where necessary;
  - The corrected draft questionnaire is sent to each focal point for final approval; and
  - The validated questionnaire is used for analysis, scoring and ranking.

A.10 The Cyber Power Index (CPI)

The Cyber Power Index (CPI) was created by the Economist Intelligence Unit research program sponsored by Booz Allen Hamilton in 2011. The CPI is a “dynamic quantitative and qualitative model, […] that measures specific attributes of the cyber environment across four drivers of cyber power: legal and regulatory framework; economic and social context; technology infrastructure; and industry application, which examines digital progress across key industries”[31]. The objective of the Cyber Power Index is to benchmark the capability of the G20 countries to withstand cyber-attacks and deploy the required digital infrastructure for a thriving and secure economy. The benchmark provided by the CPI focuses on 19 countries of the G20 (excluding the EU). The index then provides a ranking of countries for each indicator.

Attributes/ Dimensions

The Cyber Power Index (CPI) is based on four drivers of cyber power. Each category is then measured through multiple indicators to give each country a specific score. The categories and pillars are as follows:

i **Legal and Regulatory Framework**
- Government commitment to cyber development
- Cyber protection policies
- Cyber censorship (or lack thereof)
- Political efficacy
- Intellectual property protection

ii **Economic and Social Context**
- Educational levels
- Technical skills
- Openness of trade
- Degree of innovation in the business environment

iii **Technology Infrastructure**
- Access to information and communications technology
- Quality of information and communications technology
- Affordability of information and communications technology
- Spending on information technology
- Number of secure servers

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

iv Industry Application

- Smart grids
- E-Health
- E-Commerce
- Intelligent transportation
- E-Government

Assessment Method

The CPI is a quantitative and qualitative scoring model. The assessment was conducted by The Economist Intelligence Unit using quantitative indicators from available statistical sources and making estimates when data was lacking. The main sources used are the Economist Intelligence Unit; the UN Educational, Scientific and Cultural Organization (UNESCO); the International Telecommunications Union (ITU); and the World Bank.

A.11 The Cyber Power Index (CPI)

This section summarises the main findings of the analysis of the existing maturity models. Table 5: Overview of analysed maturity **models** provides an overview of the main characteristics of each model according to the modified Becker's model. Table 6 Comparison of Maturity Levels the high-level definitions of the maturity levels of the analysed models. Table 7 provides an overview of the dimensions or attributes used in each model.

Table 5: Overview of analysed maturity models

Model Name	Institution Source	Purpose	Target	Nb of Levels	Nb of attributes	Assessment Method	Results Representation
Cybersecurity Capacity Maturity Model for Nations (CMM)	Global Cybersecurity Capacity Centre University of Oxford	Increase the scale and effectiveness of cybersecurity capacity-building internationally	Countries	5	5 main dimensions	Collaboration with local organisation to fine-tune the model before applying it to the national context	Five-section radar
Cybersecurity Capability Maturity Model (C2M2)	U.S. Department of Energy (DOE)	Help organizations to evaluate and make improvements to their cybersecurity programs and strengthen their operational resilience	Organisations of all sectors, types, and sizes	4	10 main domains	Self-evaluation methodology and toolkit	Score card with pie charts
Framework for Improving Critical Infrastructure Cybersecurity	National Institute of Standards and Technology (NIST)	Framework aimed at guiding cybersecurity activities and managing risks within organisations	Organisations	N/A (4 Tiers)	5 core functions	Self-assessment	-
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	Qatar University’s College of Law	Providing a workable model that can be used to benchmark, measure and develop Qatar’s cybersecurity framework	Qatari organisations	5	5 main domains	-	-
Cybersecurity Maturity Model Certification (CMMC)	U.S. Department of Defense (DOD)	Foster Cybersecurity Best Practices to safeguard information	Defense Industrial Base sector (DIB) organisations	5	17 main domains	Assessment by third party auditors	-
The Community Cybersecurity Maturity Model (CCSMM))	Centre for Infrastructure Assurance and Security University of Texas	Determine the current status of a community in its cyber preparedness and provide a roadmap for communities to follow in their preparation efforts	Communities (local or state governments)	5	6 main dimensions	Assessment within communities with input from state and federal law enforcement agencies	-
Information Security Maturity Model for NIST Cybersecurity Framework (ISMM)	College of Computer Sciences and Engineering King Fahd University of Petroleum and, Minerals, Dhahran, Saudi Arabia	Enabling organisations to measure their implementation progress over time to ensure that they are maintaining the desired security posture	Organisations	5	23 assessed areas	-	-
Internal Audit Capability Model (IA-CM) for the Public Sector	The Institute of Internal auditors Research Foundation	Build internal audit capability and advocacy through self-assessment in the public sector	Public Sector organisations	5	6 elements	Self-assessment	-
The Global Cybersecurity Index (GCI)	International Telecommunication Union (ITU)	To review the cybersecurity commitment and situation and help countries identify areas for improvement in the field of cybersecurity	Countries	N/A	5 pillars	Self-assessment	Ranking table
The Cyber Power Index (CPI)	The Economist Intelligence Unit & Booz Allen Hamilton	To benchmark the capability of the G20 countries to withstand cyber-attacks and deploy the required digital infrastructure for a thriving and secure economy.	G20 Countries	N/A	4 categories	Benchmarking by the Economist Intelligence Unit	Ranking table

Table 6 Comparison of Maturity Levels

Model	Level 1	Level 2	Level 3	Level 4	Level 5
Cybersecurity Capacity Maturity Model for Nations (CMM)	**Start-up** Either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity-building, but no concrete actions have been taken. There is an absence of observable evidence at this stage.	**Formative** Some features of the aspects have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined – or simply "new". However, evidence of this activity can be clearly demonstrated.	**Established** The elements of the aspect are in place and working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision making has been made concerning the "relative" investment in the various elements of the aspect. However, the aspect is functional and defined.	**Strategic** Choices have been made about which parts of the aspect are important, and which are less important for the particular organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional upon the nation or organization's circumstances.	**Dynamic** There are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technology of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this stage.
Cybersecurity Capability Maturity Model (C2M2)	**MIL0** Practices are not performed.	**MIL1** Initial practices are performed but may be ad hoc.	**MIL2** Management characteristics: Practices are documented; Adequate resources are provided to support the process; Personnel performing the practices have adequate skills and knowledge; and Responsibility and authority for performing the practices are assigned. Approach characteristic: Practices are more complete or advanced than at MIL1.	**MIL3** Management characteristics: Activities are guided by policies (or other organizational directives); Performance objectives for domain activities are established and monitored to track achievement; and Documented practices for domain activities are standardized and improved across the enterprise. Approach characteristic: Practices are more complete or advanced than at MIL2.	-
Information Security Maturity Model for NIST Cyber Security Framework (ISMM)	**Performed Process**	**Managed Process**	**Established Process**	**Predictable Process**	**Optimizing Process**
Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	**Initiating** Employs ad-hoc cybersecurity practices and process under some of the domains.	**Developing** Implemented policies and practices to develop and improve cybersecurity activities under the domains with the aim of suggesting new activities to implement.	**Implementing** Adopted policies to implement all of the cybersecurity activities under the domains with the aim of completing implementation at a certain time.	**Adaptive** Revisits and reviews cybersecurity activities and adopts practices based on predictive indicators derived from previous experiences and measures.	**Agile** Continues to practice the adaptative stage with added emphasis on the agility and speed in implementing activities in the domains.

Cybersecurity Maturity Model Certification (CMMC)	**Processes: Performed** Because the organization may only be able to perform these practices in an ad-hoc manner and may or may not rely on documentation process maturity is not assessed for Level 1. **Practices: Basic Cyber Hygiene** Level 1 focuses on the protection of FCI (Federal Contract Information) and consists only of practices that correspond to the basic safeguarding requirements.	**Processes: Documented** Level 2 requires that an organization establish and document practices and policies to guide the implementation of their CMMC efforts. The documentation of practices enables individuals to perform them in a repeatable manner. Organizations develop mature capabilities by documenting their processes and then practicing them as documented. **Practices: Intermediate Cyber Hygiene** Level 2 serves as a progression from Level 1 to Level 3 and consists of a subset of the security requirements specified in NIST SP 800-171 as well as practices from other standards and references.	**Processes: Managed** Level 3 requires that an organization establish, maintain, and resource a plan demonstrating the management of activities for practice implementation. The plan may include information on missions, goals, project plans, resourcing, required training, and involvement of relevant stakeholders. **Practices: Good Cyber Hygiene**. Level 3 focuses on the protection of CUI (Controlled Unclassified Information) and encompasses all of the security requirements specified in NIST SP 800-171 as well as additional practices from other standards and references to mitigate threats.	**Processes: Reviewed.** Level 4 requires that an organization reviews and measures practices for effectiveness. In addition to measuring practices for effectiveness, organizations at this level are able to take corrective action when necessary and inform higher level management of status or issues on a recurring basis. **Practices: Proactive** Level 4 focuses on the protection of CUI (Controlled Unclassified Information) and encompasses a subset of the enhanced security requirements. These practices enhance the detection and response capabilities of an organization to address and adapt to the changing tactics, techniques, and procedures.	**Processes: Optimizing** Level 5 requires an organization to standardize and optimize process implementation across the organization. **Practices: Advanced/Proactive** Level 5 focuses on the protection of CUI (Controlled Unclassified Information). The additional practices increase the depth and sophistication of cybersecurity capabilities.
The Community Cyber Security Maturity Model (CCSMM)	**Security Aware** The major theme of activities at this level is to make individuals and organizations aware of the threats, problems, and issues related to cyber security	**Process Development** Level designed to help communities establish and improve upon the security processes required to effectively address cyber security issues.	**Information Enabled** Designed to improve upon the information sharing mechanisms within the community to enable the community to effectively correlate seemingly disparate pieces of information.	**Tactics Development** This level elements are designed to develop better and more proactive methods to detect and respond to attacks. By this level most prevention methods should be in place.	**Full Security Operational Capability** This level represents those elements that should be in place for any organization to consider itself fully operationally read y to address any type of cyber threat.
Internal Audit Capability Model (IA-CM) for the Public Sector	**Initial** No sustainable, repeatable capabilities – dependent on individual efforts	**Infrastructure** Sustainable and repeatable practices and procedures	**Integrated** Management and professional practices uniformly applied	**Managed** Integrates information from across the organization to improve governance and risk management	**Optimizing** Learning from inside and outside the organization for continuous improvement

Table 7: Comparison of Attributes/ Dimensions

	Cybersecurity Capacity Maturity Model for Nations (CMM)	Cybersecurity Capability Maturity Model (C2M2)	Qatar Cybersecurity Capability Maturity Model (Q-C2M2)	Cybersecurity Maturity Model Certification (CMMC)	Cybersecurity Maturity Model Certification (CMMC)	Information Security Maturity Model for NIST Cyber Security Framework (ISMM)	Framework for Improving Critical Infrastructure Cybersecurity	The Global Cybersecurity Index (GCI)	The Cyber Power Index (CPI)
Levels	Five dimensions divided into several factors themselves including multiple aspects and indicators (Figure 4)	Ten domains, including a unique management objective and several approach objectives (Figure 6)	Five domains divided into subdomains	Seventeen domains detailed into processes and one to many capabilities which are then detailed into Practices (Figure 9).	Six main dimensions	Twenty-three assessed areas	Five Functions with underlying key Categories and Subcategories (Figure).	Five pillars including several indicators	Four categories with several indicators

Attributes/ Dimensions	i Devising cybersecurity policy and strategy;
	ii Encouraging responsible cybersecurity culture within society;
	iii Developing cybersecurity knowledge;
	iv Creating effective legal and regulatory frameworks; and
	v Controlling risks through standards, organisations and technologies.
		i Risk Management;
		ii Asset, Change, and Configuration Management;
		iii Identity and Access Management;
		iv Threat and Vulnerability Management;
		v Situational Awareness;
		vi Event and Incident Response;
		vii Supply Chain and External Dependencies Management;
		viii Workforce Management;
		ix Cybersecurity Architecture;
		x Cybersecurity Program Management.
			i Understand (Cyber governance, Assets, Risks, and Training);
			ii Secure (Data Security, Technology Security, Access Control Security, Communications Security, and Personnel Security);
			iii Expose (Monitoring, Incident Management, Detection, Analysis, and Exposure);
			iv Respond (Response Planning, Mitigation, and Response Communication);
			v Sustain (Recovery Planning, Continuity Management, Improvement, and External Dependencies).
				i Access Control;
				ii Asset Management;
				iii Audit and Accountability;
				iv Awareness and Training;
				v Configuration Management;
				vi Identification and Authentication;
				vii Incident Response;
				viii Maintenance;
				ix Media Protection;
				x Personnel Security;
				xi Physical Protection;
				xii Recovery;
				xiii Risk Management;
				xiv Security Assessment;
				xv Situational Awareness;
				xvi System and Communications Protection;
				xvii System and Information Integrity.
					i Threats Addressed;
					ii Metrics;
					iii Information Sharing;
					iv Technology;
					v Training;
					vi Test.
						i Asset Management;
						ii Business Environment;
						iii Governance;
						iv Risk Assessment;
						v Risk Management Strategy;
						vi Compliance Assessment;
						vii Access Control;
						viii Awareness and Training;
						ix Data Security;
						x Information Protection Processes and Procedures;
						xi Maintenance;
						xii Protective Technology;
						xiii Anomalies and Events;
						xiv Security Continuous Monitoring;
						xv Detection Processes;
						xvi Response Planning;
						xvii Response Communications;
						xviii Response Analysis;
						xix Response Mitigation;
						xx Response Improvements;
						xxi Recovery Planning;
						xxii Recovery Improvements;
						xxiii Recovery Communications.
							i Identify;
							ii Protect;
							iii Detect;
							iv Respond;
							v Recover.
								i Legal;
								ii Technical;
								iii Organizational;
								iv Capacity-building;
								v Cooperation.
									i Legal and Regulatory Framework;
									ii Economic and Social Context;
									iii Technology Infrastructure;
									iv Industry Application.

ANNEX B – DESK RESEARCH BIBLIOGRAPHY

Almuhammadi, S. and Alsaleh, M. (2017) ‘Information Security Maturity Model for Nist Cyber Security Framework’, in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. and Alsaleh, M. (2017) ‘Information Security Maturity Model for Nist Cyber Security Framework’, in Computer Science & Information Technology (CS & IT). Available at: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Available at: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgian Government (2012) Cyber Security Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. RAND Corporation. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012) ‘Introduction to Return on Security Investment’.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) “Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Available at https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Available at : https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Council of Ministers (2019) Portuguese Official Journal, Series 1 — No. 108 - Resolution of the Council of Ministers No. 92/2019. Available at: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). University of Oxford.

CSIRT Maturity - Self-assessment Tool (no date). Available at: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011)

Specialised cybercrime units - Good practice study. Available at: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Cybersecurity Incident Report and Analysis System – Visual Analysis Tool (no date). Available at: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (no date) 'Welcome to the NCSS Training Tool'.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Available at: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Available at: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Available at: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016) Cybersecurity Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design - from policy to engineering.* Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

European Commission (2012) Regulation of the European parliament and of the council on electronic identification and trust services for electronic transactions in the internal market. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

European Network and Information Security Agency (2012) NCSS: Practical Guide on Development and Execution. Heraklion: ENISA.

European Network and Information Security Agency (2012) NCSS: Setting the course for national efforts to strengthen security in cyberspace. Heraklion: ENISA.

European Network and Information Security Agency (2016) Guidelines for SMEs on the security of personal data processing.

European Network and Information Security Agency (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Heraklion: ENISA.

European Union and Agency for Network and Information Security (2017) Handbook on security of personal data processing. Available at: http://dx.publications.europa.eu/10.2824/569768

European Union and Agency for Network and Information Security (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Available at: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Executive Office Of The President (2015) Memorandum for Heads of Executive Departments and Agencies. Available at: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Federal Chancellery of the Republic of Austria (2013) Austrian Cyber Security Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Federal Ministry of the Interior (2011) Cyber Security Strategy for Germany. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

French Prime Minister's Office (2014) French National Digital Security Strategy. Available at: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) 'Evaluating Business Process Maturity Models', Journal of the Association for Information Systems. Available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Government of Bulgaria (2015) National Cyber Security Strategy - Cyber-resistant Bulgaria 2020.

Government of Croatia (2015) The National Cyber Security Strategy of The Republic of Croatia. Available at: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Government of Greece (2017) National Cyber Security Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Government of Hungary (2018) Strategy for the Security of Network and Information Systems. Available at: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Government of Ireland (2019) National Cyber Security Strategy. Available at: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Government of Spain (2019) National Cyber Security Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Institute of Internal Auditors (ed.) (2009) Internal audit capability model (IA-CM) for the public sector: overview and application guide. Altamonte Springs, Fla: Institute of Internal Auditors, Research Foundation.

International Telecommunication Union (ITU) (2018) The Global Cybersecurity Index. Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

International Telecommunication Union (ITU) (2018) Guide to developing a national cybersecurity strategy. Available at: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) 'Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework', International Review of Law.

Latvian Government (2014) Cyber Security Strategy of Latvia. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Heraklion: ENISA. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Ministry for Competitiveness and Digital, Maritime and Services Economy (2016) Malta Cyber Security Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Ministry of Economic Affairs and Communications (2019) Cybersecurity Strategy – Republic of Estonia. Available at: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Ministry of National Defence Republic of Lithuania (2018) National Cyber Security Strategy

National Cyber Security Centre (2015) National Cyber Security Strategy of the Czech Republic. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

National Cyber Security Strategies - Interactive Map (no date). Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

National Cybersecurity Strategies Evaluation Tool (2018). Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: National Institute of Standards and Technology. Available at: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Available at: https://www.omg.org/spec/BPMM/1.0/PDF

OECD, European Union and Joint Research Centre - European Commission (2008) Handbook on Constructing Composite Indicators: Methodology and User Guide. OECD. Available at: https://www.oecd.org/sdd/42495745.pdf.

Office of the commissioner of Electronic Communications and Postal Regulations (2012) Cybersecurity Strategy of the Republic of Cyprus.

Official Journal of the European Union (2008) COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Organisation for Economic Co-operation and Development (OECD) (2012) Cybersecurity policy making at a turning point. Available at: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) ‘National Cyber Security Strategies - Practical Guide on Development and Execution’.

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects

Presidency of the Council of Ministers (2017) The Italian Cybersecurity Action Plan. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019) Dziennik Urzędowy Rzeczypospolitej Polskiej. Available at: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Romanian Government (2013) Cyber security strategy of Romania. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. and European Union Agency for Cybersecurity (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Available at: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Secretariat of the Security Committee (2019) Finland’s Cyber Security Strategy 2019. Available at: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Slovakian Government (2015) Cyber Security Concept of the Slovak Republic. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015) Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010

Smith, R. (2016) ‘Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010’, in Smith, R., Core EU Legislation. London: Macmillan Education. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Swedish Government (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

The Danish Government - Ministry of Finance (2018) Danish Cyber and Information Security Strategy. Available at: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

The Federal Council (2018) National strategy for the protection of Switzerland against cyber risks.

The Luxembourguish Government Council (2018) National Cybersecurity Strategy. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

The Netherlands Governement (2018) National Cyber Security Agenda. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

The White House (2018) National Cyber Strategy of the United States of America. Available at: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) Cyber Europe Report. Available at: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. and European Network and Information Security Agency (2013) *National-level risk assessments: an analysis report.* Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Available at: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

UK National Cyber Security Strategy 2016-2021 (2016). Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

University of Innsbruck et al. (2009) Understanding Maturity Models.

Wamala, D. F. (2011) 'ITU National Cybersecurity Strategy Guide. Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) 'The Community Cyber Security Maturity Model', in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)

ANNEX C – OTHER OBJECTIVES STUDIED

The objectives detailed below were studied as part of the desk research phase and the interviews conducted by ENISA. The following objectives are not part of the National Capabilities Assessment Framework, but they shine a light on topics that are worth discussing. Each of the following sub-chapters will provide an explanation as to why the objective was discarded.

- Develop sector-specific cybersecurity strategies;
- Fight against disinformation campaigns;
- Secure cutting-edge technologies (5G, AI, quantum computing…);
- Ensure data sovereignty; and
- Provide incentives for the development of the cyber insurance industry.

Develop sector-specific cybersecurity strategies

The adoption of sector-specific strategies that target sector interventions and incentives certainly introduces a stronger decentralised capability. It is particularly fitting for Member States whose OES's must deal with different frameworks and regulations and where there are many dependencies due to the transversal nature of cybersecurity. Indeed, in several Member States, it is common to count dozens of national authorities and regulatory bodies with knowledge of each sector's specificities that hold a mandate to enforce specific regulation for each sector.

Denmark, for example, launched six targeted strategies addressing the most critical sectors' cyber and information security efforts to develop a stronger decentralised capability in cyber and information security. Each 'sectoral unit' will contribute to threat assessments at sectoral level, monitoring, preparedness exercises, establishment of security systems, knowledge-sharing and instructions, among others. The sector-specific strategies cover the following sectors:

- Energy;
- Healthcare;
- Transport;
- Telecommunication;
- Finance; and
- Maritime.

Other Member States have expressed interest in considering sector-specific cybersecurity strategies to reflect all regulatory requirements. However, it must be noted that such an objective might not fit all Member States depending on their size, national policies and maturity. The great difficulty to ensure that the framework can account for all specificities led ENISA to not include this objective in the framework.

Fight against disinformation campaigns

Member States integrate the protection of fundamental principles such as human rights, transparency and public trust into their national cybersecurity strategies. This is very important especially when it comes to disinformation that is disseminated via traditional news media or social media platforms. In addition, cybersecurity is currently one of the greatest electoral challenges. Indeed, activities such as spreading false information or negative propaganda have been observed in various countries in the run-up to important elections. This threat has the potential to undermine the EU democratic process. At the European level, the Commission has outlined an Action Plan[32] to step up efforts to counter disinformation in Europe: this plan focuses on 4 key areas (detection, cooperation, collaboration with online platforms and awareness) and serves to build the EU's capabilities and strengthen cooperation between Member States.

4 out of 19 interviewed countries have expressed their intent to tackle the issue of disinformation and propaganda in their NCSS.

For example, the French NCSS[33] notes that: "it is the State's responsibility to inform citizens of the risks of manipulation and propaganda techniques used by malicious players on the Internet. For example, after the terrorist attacks against France in January 2015, the Government established an information platform on the risks related to Islamic radicalisation via electronic communication networks: « Stop-djihadisme.gouv.fr »." This approach could be extended to respond to other phenomena of propaganda or destabilisation.

In another example, Poland's 2019-2024 NCSS[34] states that: "against manipulative activities such as disinformation campaigns, systemic actions are needed to develop citizens' awareness in the context of verifying the authenticity of information and responding to attempts to distort it."

However, during interviews conducted by ENISA, several Member States shared that they do not address the issue as part of their NCSS as a cybersecurity threat but rather tackle the issue at a broader societal level, for example, via policy initiatives.

Secure cutting-edge technologies (5G, AI, quantum computing…)

As the current cyber threat landscape continues to expand, the development of new technologies will most probably result in an increase in the intensity and number of cyber-attacks and the diversification of methods, means and targets employed by threat actors. In the meantime, these new technological solutions in the form of cutting-edge technologies have the potential to become the building blocks of the European Digital Market. In order to safeguard Member States' growing digital dependency and the emergence of new technologies, incentives and fully-fledged policies should be established to support the secure and trustworthy development and deployment of these technologies in the EU.

During the desk research phase performed on Member States' NCSS's, the following cutting-edge technologies were put forward as being of interest to the Member States: 5G, AI, quantum computing, cryptography, edge computing, connected and autonomous vehicles, big and smart data, blockchain, robotics and IoT.

More particularly, in early 2020, the European Commission published a communication calling on Member States to take steps to implement the set of measures recommended in the 5G toolbox conclusions[35]. This 5G toolbox comes in the wake of Recommendation (EU) 2019/534 on the cybersecurity of 5G networks adopted by the Commission in 2019, which called for a unified European approach to the security of 5G networks[36].

During interviews conducted by ENISA, it was highlighted that this topic is more of a transversal topic which is addressed across the NCSS rather than as a specific objective *per se*.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35]https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

Ensure data sovereignty

On the one hand, cyberspace can be seen as a formidable global common space, which is easily accessible, providing a high degree of connectivity and able to yield great opportunities for socio-economic growth. On the other hand, cyberspace is also characterized by its weak jurisdiction, difficulty to attribute actions, lack of frontiers, and interconnected systems which can be porous and whose data can be stolen or even accessed by foreign governments. In addition to these two perspectives, the digital ecosystem is marked by the concentration of online service platforms and infrastructure in the hands of very few stakeholders. All aspects aforementioned lead Member States to promote digital sovereignty. Achieving digital sovereignty means that citizens and businesses are able to fully thrive by using digital services and ICT products that are trustworthy without any fear for one's personal data, or digital assets, one's economic autonomy or one's political influence.

Data sovereignty or digital sovereignty is championed by Member States at the national level and at the European level. While Member States do not seem to address the issue directly in their NCSS as a specific objective, they either address it as a transversal principle or they outline their intention to ensure digital sovereignty at national level outline in *ad hoc* publications by focusing on key technologies. For example, in the 2018 French strategic review of cyber defence, it is stated that "controlling the following technologies are of paramount importance to ensure digital sovereignty: communication encryption, cyber-attack detection, professional mobile radio, cloud computing and artificial intelligence"[37].

At the European level, Member States are actively participating in defining the European strategy for Data (COM/2020/66 final) and building the EU certification framework for ICT digital products, services and processes established by the EU Cybersecurity Act (2019/881) to ensure strategic digital autonomy at European level.

The interview phase with Member States showed that the topic of digital sovereignty is often considered as a broader issue than one which is restricted to cybersecurity. Therefore, Member States do not cover the topic in their NCSS's and for the few who do, they do not cover it as a specific objective *per se*.

Provide incentive to the development of the cyber insurance industry

The current state of play of the cyber insurance industry shows that the global market has undisputedly grown. However, it is still in its early days as data must be collected and many precedents must still be set (*e.g.* silent coverage, systemic cyber risks…). Furthermore, the estimated losses aggregated from cyber-attacks around the globe are several orders of magnitude higher than the current cyber insurance industry coverage capacity (IMF Working Paper - Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment WP/18/143). However, developing the cyber insurance industry can certainly yield benefits and lay the foundation for virtuous mechanisms. Indeed, cyber insurance mechanisms can help in:

- Raising awareness about cybersecurity risks in companies;
- Evaluating the exposure to cyber risks in quantitative manner;
- Improving cybersecurity risk management;
- Providing support to organisations that are victims of cyber-attacks; and
- Covering the damage (material or not) induced by a cyber-attack.

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Certain Member States started to work on this topic. For example:

- Estonia adopted a "wait and see" approach in their NCSS: "To mitigate cyber risks in the private sector in general, demand and supply of cyber insurance service in Estonia will be analysed and on that basis, cooperative principles for related parties will be agreed upon, including information sharing, preparation of risk assessment, etc. Today, suppliers of cyber insurance service are few on the Estonian market and it is necessary to first map who offers what. The complexity of insurance protection is often considered a hindrance to the development of the cyber insurance market."
- Luxembourg specifically supports the development of the cyber insurance industry in its NCSS: ”Objective 1: Creating new products and services. To pool risks and encourage victims of digital cyber incidents to seek help from experts to manage the incident and restore a system affected by a malicious act, insurance companies will be encouraged to create specific products for the area of cyber insurance."

Feedbacks from interviewees were quite diverse on this topic: some Member States stated that the cyber insurance topic has recently become a topic of discussion, while others shared that although the topic is promising, the industry is not mature enough yet. However, a great number of interviewees declared that the topic is not tackled as part of the NCSS, either because it was deemed to be too specific or not within the scope of the NCSS.

TP-06-20-047-EN-N

About the European Union Agency for Cybersecurity

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. For more information, visit www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN: 978-92-9204-443-5
DOI: 10.2824/590072