TLP - CLEAR

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

National Capabilities Assessment Framework 2.0

National Capabilities Assessment Framework – 2026 Edition

APRIL 2026

About ENISA

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

CONTACT

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

LEGAL NOTICE

Luxembourg: Publications Office of the European Union, 2026

COPYRIGHT NOTICE

ISBN 978-92-9204-789-4, DOI 10.2824/5812948

USE OF AI-ASSISTED TOOLS

AI-assisted tools were used in a limited capacity to support language refinement, terminology alignment, translation and preliminary document screening. All outputs were reviewed and validated by subject-matter experts. No AI-generated content was used without substantive human oversight.

Table of Contents

Glossary of Terms

Acronym	Definition
ACP	Active Cyber Protection
AI	Artificial Intelligence
BGP	Border Gateway Protocol
BRP	Business Recovery Plan
C2M2	Cybersecurity Capability Maturity Model
CCDCoE	Cooperative Cyber Defence Centre of Excellence
CDEP	Committee on Digital Economy Policy
CDI	Cyber Defence Index
CEF	Connecting Europe Facility
CER Directive	Critical Entities Resilience Directive
CI	Critical infrastructure
CIIP	Critical Information Infrastructure Protection
CIRAS	Cybersecurity Incident Response and Analysis System
CMM	Cybersecurity Capacity Maturity Model for Nations
CMMC	Cybersecurity Maturity Model Certification
COBIT	Control Objectives for Information and related Technology
CRA	Cyber Resilience Act
CSoA	Cyber Solidarity Act
CSIRT	Computer Security Incident Response Teams
CVD	Coordinated Vulnerability Disclosure
DEP	Digital Europe Programme
DNS	Domain Name System
DORA	Digital Operational Resilience Act
DPIA	Data Protection Impact Assessment
ECCC	European Cybersecurity Competence Centre
ECCG	European Cybersecurity Certification Group
ECSF	European Cybersecurity Skills Framework
ECSM	European Cybersecurity Month
EDIH	European Digital Innovation Hubs

Acronym	Definition
EDR	Endpoint Detection and Response
EEAS	European External Action Service
EU-CSI	EU Cybersecurity Index
EU-Cyclone	European Cyber Crisis Liaison Organisation Network
Eurojust	European Union Agency for Criminal Justice Cooperation
Europol	European Union Agency for Law Enforcement Cooperation
EC3	European Cybercrime Centre
FIRST	Forum of Incident Response and Security Teams
GCI	Global Cybersecurity Index
GDPR	General Data Protection Regulation
GFCE	Global Forum on Cyber Expertise
HR	Human Resources
IA-CM	Internal Audit Capability Model
ICS2	International Information System Security Certification Consortium
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IPR	Incident Preparedness and Response
ISACs	Information Sharing and Analysis Centres
ITU	International Telecommunication Union
LEA	Law Enforcement Agency
LED	Law Enforcement Directive
LLMs	Large Language Models
MFA	Multifactor authentication
MS	Member State
NATO	North Atlantic Treaty Organisation
NCAF	National Capabilities Assessment Framework
NCC	National Coordination Centre
NCCA	National Cybersecurity Certification Authority
NCSS	National Cybersecurity Strategy
NIS2	Network and Information Security Directive 2
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development

Acronym	Definition
OSCE	Organisation for Security and Co-operation in Europe
PET	Privacy Enhancing Technologies
PoC	Point of Contact
PPP	Public-private partnership
R&D	Research & Development
SMEs	Small and medium-sized enterprises
SOC	Security Operation Centre
SOP	Standard Operating Procedures
SPOC	Single Point of Contact
TF-CSIRT	Task Force – Computer Incident Response Teams

Executive Summary

As cybersecurity threats continuously expand and intensify and the legislative landscape of the European Union evolves to tackle these cybersecurity challenges, EU Member States need to react effectively by developing and adapting their national cybersecurity strategies (NCSSs). Since 2017, all Member States have had an NCSS. However, the development of a comprehensive NCSS is a challenging and complex process. To support the Member States in the development and implementation of their NCSSs, the European Union Agency for Cybersecurity (ENISA) published a national capabilities assessment framework (NCAF) in 2020. This report represents an updated version (NCAF 2.0) of the framework, which reflects how the threat landscape has evolved and the advancements in legislation since the earlier version.

The framework aims to help Member States to undertake a self-assessment of their level of maturity by assessing their NCSS objectives. This will help them to enhance and build cybersecurity capabilities at both the strategic and the operational levels, thereby strengthening the collective cybersecurity posture across the EU.

The NCAF is a tool that helps Member States by:

- providing useful information to help them develop a long-term strategy (e.g., good practices and guidelines);
- helping them to identify missing elements within their NCSSs;
- helping them to further build their cybersecurity capabilities;
- supporting the accountability of political actions;
- giving credibility to their NCSSs from the perspective of the general public and international partners;
- supporting outreach and increasing transparency, thus enhancing the public image of participating organisations;
- helping them to anticipate the issues lying ahead;
- helping them to identify lessons learned and best practices;
- providing a baseline on cybersecurity capacity across the EU to facilitate discussions;
- helping them to evaluate national capabilities regarding cybersecurity.

The target audience of this report is policymakers, subject-matter experts and government officials engaged in the design, implementation and evaluation of NCSSs and, more broadly, cybersecurity capabilities.

The NCAF 2.0 covers 20 strategic objectives and is structured around **four main clusters**:

Cluster #1: Capacity-building and awareness	**OBJECTIVE #1** Strengthen the Cyber-Resilience and Hygiene of Private Sector, Including SMEs	**OBJECTIVE #2** Promote Cybersecurity Awareness and cyber-hygiene on cybersecurity	**OBJECTIVE #3** Address the Cybersecurity Skills Gap	**OBJECTIVE #4** Foster Research and Development (R&D) and Innovation	**OBJECTIVE #5** Enhance Incident Preparedness and Response
Cluster #2: Cooperation and collaboration	**OBJECTIVE #6** Address cybercrime	**OBJECTIVE #7** Engage in international cooperation	**OBJECTIVE #8** Establish trusted information - sharing and mechanisms	**OBJECTIVE #9** Establish mutual assistance processes	**OBJECTIVE #10** Develop crisis management frameworks
Cluster #3: Cybersecurity governance	**OBJECTIVE #11** Secure digital identity and build trust in digital public services	**OBJECTIVE #12** Establish national level risk-assessment	**OBJECTIVE #13** Strengthen national cybersecurity governance	**OBJECTIVE #14** Establish cybersecurity risk-management measures	**OBJECTIVE #15** Establish incident reporting mechanisms
Cluster #4: Regulatory and policy frameworks	**OBJECTIVE #16** Balance security with privacy	**OBJECTIVE #17** Improve the cybersecurity of the supply chain	**OBJECTIVE #18** Protect critical sectors	**OBJECTIVE #19** Establish a CVD policy	**OBJECTIVE #20** Promote active cyber protection

SECTION 1

Introduction

1. Introduction

The Network and Information Security Directive (NIS2) [1], which entered into force in January 2023, aims to strengthen the resilience and security of network and information systems across the European Union. It obliges EU Member States to establish comprehensive national strategies for cybersecurity – referred to as national cybersecurity strategies (NCSSs) – in accordance with its updated provisions. An NCSS, within the scope of NIS2, represents a structured framework that articulates strategic principles, objectives, priorities, policies and regulatory measures, collectively ensuring a robust and sustainable level of cybersecurity. The overarching intention of these strategies is not only to mitigate present and emerging threats to network and information systems, but also to foster innovation and support the economic and social advancement of Member States.

Within this evolving legislative landscape, the European Union Agency for Cybersecurity (ENISA) plays a pivotal role in promoting the harmonisation and continual improvement of NCSS development and implementation. In line with the EU Cybersecurity Act [2], ENISA supports Member States in adopting and executing NIS2 alongside other key cybersecurity-related legislation, such as the Cyber Resilience Act (CRA) [3] and the Digital Operational Resilience Act (DORA) [4], by sharing best practices, providing methodological guidance and gathering insights from national experiences.

To aid Member States in developing NCSSs, ENISA published the national capabilities assessment framework (NCAF) [5] in 2020. The NCAF aims to support Member States in measuring and enhancing the maturity of their NCSSs, thereby strengthening the collective cybersecurity posture across the EU. Since then, the evolving threat landscape and advancements in legislation have necessitated an update to the framework. This update brings the NCAF in line with NIS2. The update to the NCAF primarily consists of:

- updating the maturity model, including descriptions of maturity levels;
- revising the clustering of strategic objectives and developing goals for revised strategic objectives;
- developing a comprehensive set of new maturity questions across the maturity levels and strategic objectives.

1.1 Study scope and objectives

The main objective of this study is to update the NCAF, referred to as NCAF 2.0, a tool designed to help Member States to measure the maturity of their cybersecurity capabilities. Specifically, the framework should empower the Member States to:

- conduct the evaluation of their national cybersecurity capabilities;
- enhance awareness of their cybersecurity maturity level;

(1) https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.
(2) https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.
(3) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32024R2847.
(4) https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.
(5) https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework.

- identify priority areas for improvement;
- strengthen and build cybersecurity capabilities.

This framework is intended to assist Member States, particularly national policymakers, in performing a self-assessment exercise aimed at improving national cybersecurity capabilities.

1.2 Methodological approach

NCAF 2.0 was developed using a methodological approach consisting of the following main steps:

- conducting desk research using publicly available sources;
- updating the NCAF maturity model;
- conducting a survey to validate the updated maturity model and the maturity questions for three prioritised objectives;
- developing maturity questions for the updated NCAF objectives;
- reviewing feedback from Member States collected during the survey and development of the first draft of NCAF 2.0;
- organising a validation workshop with Member States;
- finalising NCAF 2.0.

1.2.1 Desk research of publicly available sources

The first step involved conducting a comprehensive review of publicly available sources. A full list of the material reviewed is provided in Annex A. The main sources included:

- NCSSs;
- cybersecurity-related EU law and directives and other relevant documents published by EU institutions;
- maturity models.

First, the desk research focused on the NCSSs and related national documents – such as implementation and action plans – from all Member States and from closely cooperating countries including Liechtenstein, Norway and Switzerland. Although the analysis included strategies available at the time of the original NCAF publication, special attention was given to the documents published since its publication in 2020. The primary goal of reviewing the NCSSs and related national documents was to gain insight into how the objectives set out by ENISA in the NCAF, as well as the national cybersecurity priorities and practices of individual Member States, were implemented.

In the second step of the desk research, relevant cybersecurity EU regulations and other documents published by EU institutions – such as studies and reports – were analysed. The analysis primarily focused on key cybersecurity-related documents in the EU legislative

landscape, as featured in the *2024 Report on the State of Cybersecurity in the Union* ([6]), including NIS2 [7], the Cybersecurity Act [8], the CRA [9] and DORA [10]. Subsequently, other relevant publications from EU institutions were reviewed, such as *Cybersecurity roles and skills for NIS2 essential and important entities* [11], *Cybersecurity of 5G Networks* [12] and *Undersea Cables – What is at stake?* [13].

The review of national- and EU-level documents supported the formulation of new maturity questions in NCAF 2.0.

The final step of the desk research focused on publicly accessible maturity models, either recently published or updated since the publication of the NCAF in 2020. A list of these models, together with their review, is provided in **Annex B**. The analysis of the new or updated maturity models served as a key input for the revision of the NCAF maturity model.

1.2.2 Update to the national capabilities assessment framework maturity model

In the next phase, the NCAF maturity model was revised to reflect significant changes in the EU cybersecurity landscape since 2020, while retaining the original methodological framework. Updates included incorporating the new requirements for NCSSs and peer reviews under NIS2, revising the descriptions of the five maturity levels and reorganising the clustering of ENISA's strategic objectives developed for the NCSS map ( ) (see Section 2.2).

1.2.3 Survey

Once the framework update was concluded, a survey was designed to ensure that the updated NCAF aligned with Member States' needs and expectations. The survey comprises four main parts:

- a description of the updated maturity levels (see Section 2.1);
- the revised set of goals for the NCSS objectives (see Section 2.3);
- the proposed new clustering of strategic objectives (see Section 2.4);
- maturity questions for three selected objectives: objective 13 ('Strengthen national cybersecurity governance'), objective 14 ('Establish cybersecurity risk-management measures') and objective 17 ('Improve the cybersecurity of the supply chain').

The input collected by Member States served to validate these four elements of NCAF 2.0 and to inform the next steps in developing the revised framework. In total, 14 Member States completed the survey.

(6) https://enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf.
(7) https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng.
(8) https://eur-lex.europa.eu/eli/reg/2019/881/oj.
(9) https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32024R2847.
(10) https://eur-lex.europa.eu/eli/reg/2022/2554/oj/eng.
(11) https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities.
(12) https://digital-strategy.ec.europa.eu/en/library/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.
(13) https://www.enisa.europa.eu/publications/undersea-cables.

1.2.4 Development of maturity questions

The update of the NCAF maturity model guided the development of maturity questions in the next phase. The goals of each objective, as described in Section 2.3, were further developed into more granular subgoals, detailing the activities necessary to achieve the objectives. Maturity questions were then formulated for each subgoal and maturity level, ensuring comprehensive coverage of different levels of maturity across all topics. These questions were based on both EU-level legislation and other relevant documents, as well as on best practices and activities in the Member States, as described in the NCSSs and action plans. This process was initially applied to the three strategic objectives included in the survey and later extended to the remaining 17 strategic objectives.

1.2.5 Reviewing feedback from Member States collected during the survey and development of the first draft of NCAF 2.0

In parallel with the development of maturity questions, feedback from the Member States collected during the survey was reviewed and incorporated into the relevant sections of NCAF 2.0. The updated maturity levels, the revised set of goals for the objectives and the new clustering, together with the maturity questions developed for all 20 objectives, were integrated into the first draft of NCAF 2.0.

1.2.6 NCAF 2.0 piloting and feedback by Member States

The first draft of NCAF 2.0 was piloted with Greece, Italy and Luxembourg to assess its effectiveness in supporting the development and revision of the NCSSs. Overall, the pilot confirmed the practical relevance and added value of the framework. Luxembourg highlighted the usefulness of NCAF 2.0 in promoting a structured approach to NCSS preparation, particularly through the systematic mapping of existing frameworks, legislation and practices, including the minimum requirements set out in Article 7, supported by appropriate institutional coordination. Luxembourg also emphasised the need for simplification of the framework. Greece underlined the strong alignment of the framework with NIS2 and its effectiveness in mapping national and governmental policies; in identifying strengths, gaps and overlaps; and in supporting implementation planning, resource allocation and interinstitutional coordination, including in public administrations with limited resources. In this context, Greece considered that the framework is well suited to supporting a structured approach to future strategic planning and prioritisation. Italy considered that NCAF 2.0 provides valuable strategic input for the forthcoming policy cycle, notably by supporting improved prioritisation, clearer timelines and the establishment of benchmarks. Considering the NCAF 2.0 objectives, Italy also provided constructive feedback and proposals to strengthen its methodology, to simplify it and to ensure complementarity with the EU Cybersecurity Index (EU-CSI).

1.2.7 An engaging session with Member States

A world cafe session was organised to gather feedback on NCAF 2.0 through structured, practice-oriented discussions with representatives from Member States. The session provided a collaborative forum in which participants shared national best practices for implementing cybersecurity objectives and assessed whether the proposed NCAF maturity-level questions accurately reflected operational realities.

Working in groups, participants examined the goals for selected objectives, evaluating their coherence, completeness and clarity. Particular attention was paid to the relevance and practical

applicability of the maturity level-3 questions. Participants discussed national implementation examples to determine whether additional questions should be included or existing questions should be removed, in order to better capture emerging practices across Member States.

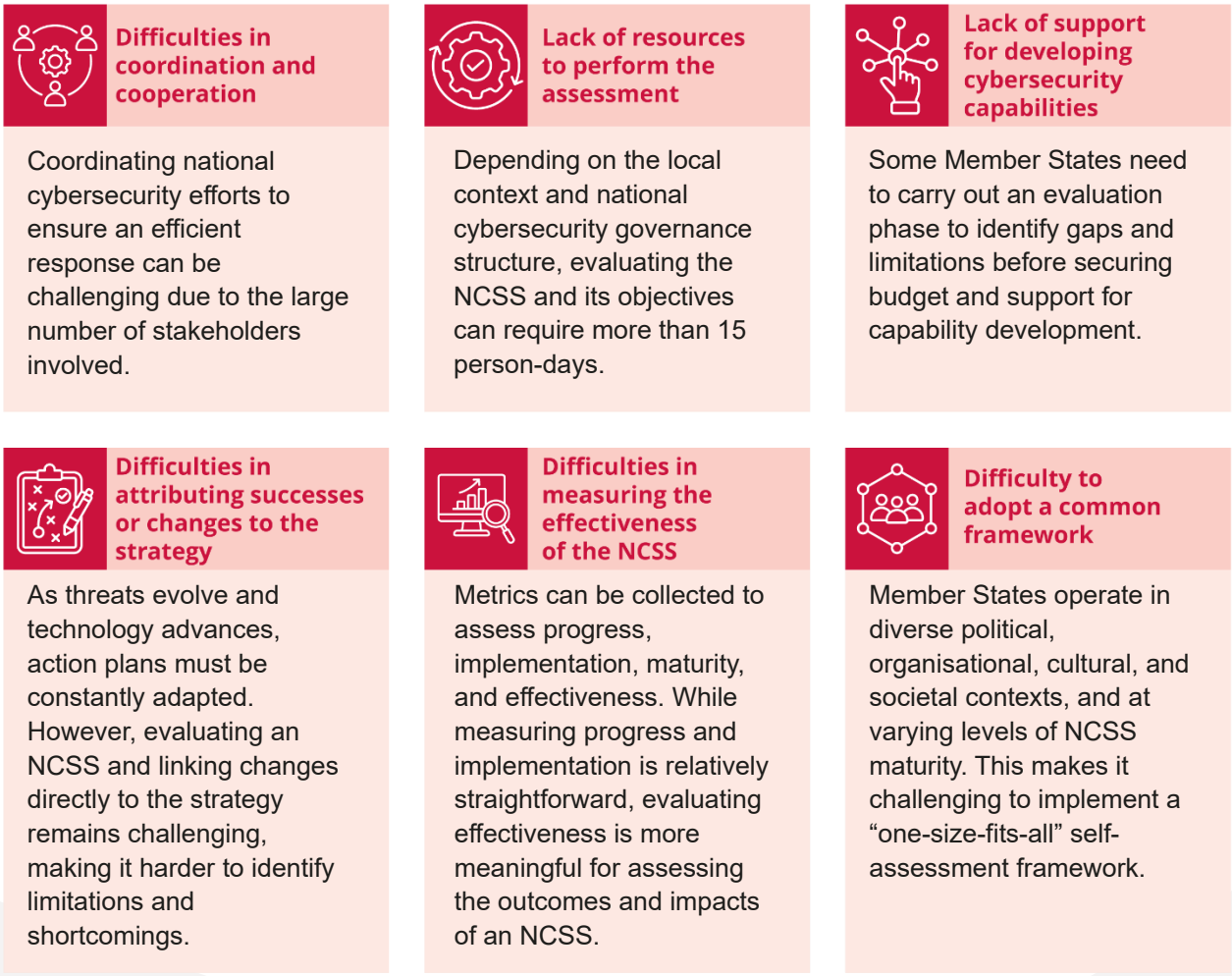
Key insights and recommendations from each group were documented by rapporteurs and presented during a plenary session. These contributions were subsequently integrated into this version of NCAF 2.0, helping to ensure that the framework remains practical, grounded in real-world experience and effective in supporting both national and collective cybersecurity capabilities across the EU.

1.3 Target audience

The primary audience of this report comprises policymakers, subject-matter experts and government officials engaged in the design, implementation and evaluation of NCSSs and, more broadly, national cybersecurity capabilities. Additionally, the findings set out in this document can be of value to cybersecurity policy experts and researchers at both the national and the European levels.

1.4 Challenges of national cybersecurity strategy evaluation

Member States face numerous challenges when building cybersecurity capabilities particularly in ensuring that these capabilities remain aligned with the latest developments. Below is a summary of the challenges identified by Member States:



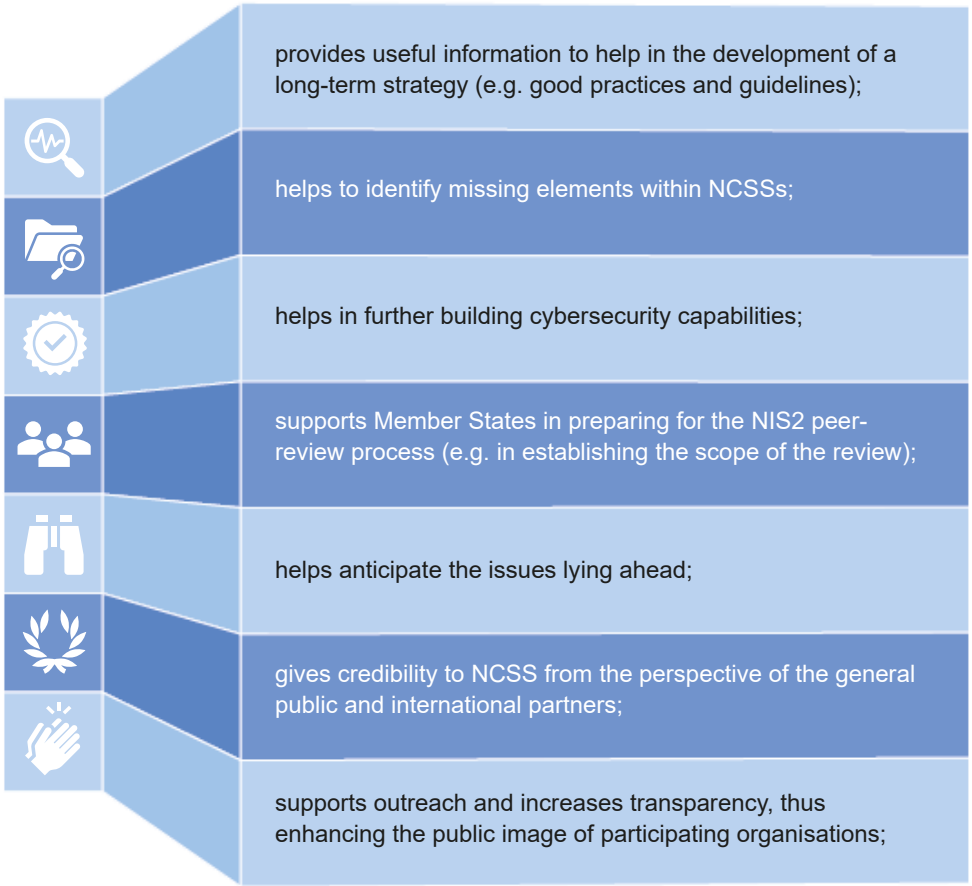
1.5 Benefits of a national capabilities assessment

Since 2017, all Member States have had an NCSS. While this is a positive development, it is also important that Member States are able to properly assess these NCSSs and thus bring added value to their strategic planning and implementation.

One of the goals of NCAF 2.0 is to evaluate cybersecurity capabilities based on the priorities set forth in the various NCSSs. 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 Member State policymakers in framing national strategies on cybersecurity by providing them with national-level intelligence on the state of play. NCAF 2.0 is ultimately intended to help Member States identify areas of improvement and build capabilities. The revised framework also takes into account recent regulatory frameworks such as NIS2 (e.g., Articles 7, 19, 21 and 23), the CRA and others, helping Member States to identify areas for improvement and strengthen their cybersecurity capabilities.

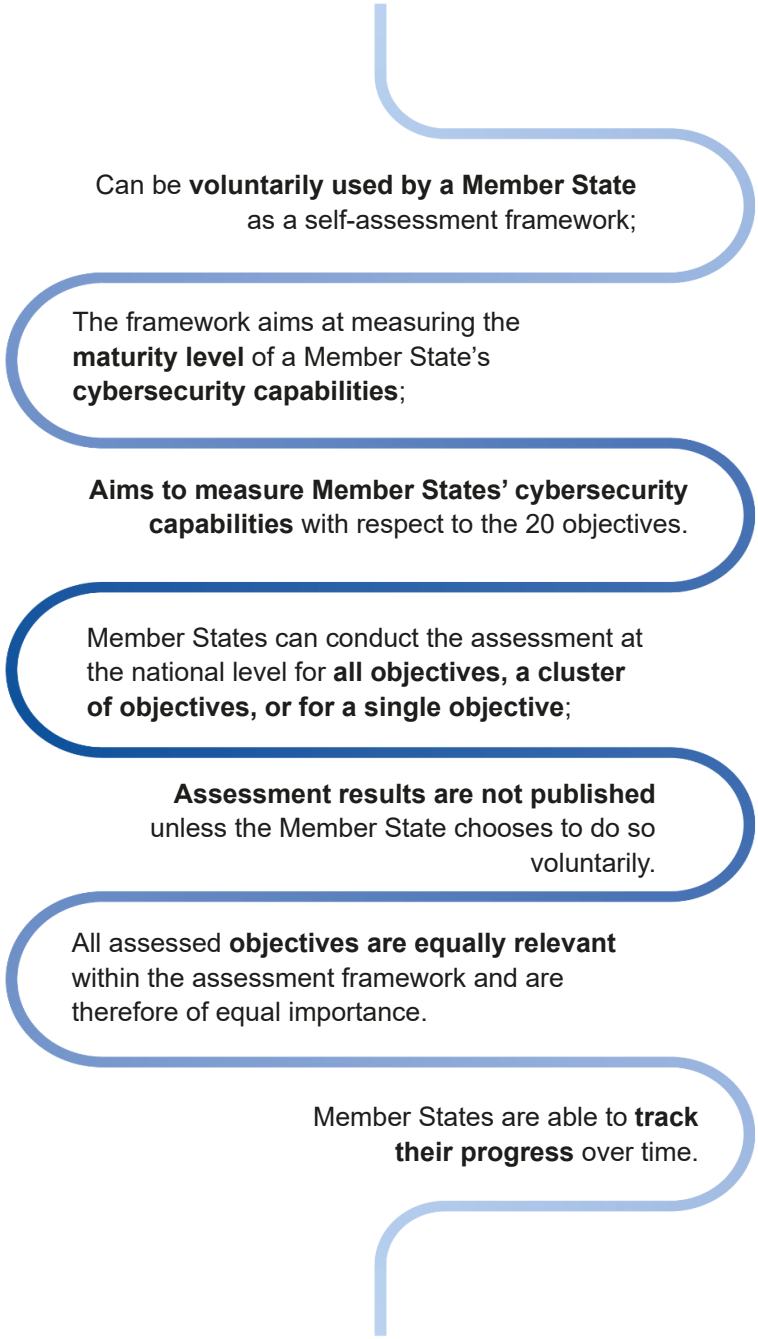
The framework aims to help Member States to undertake a self-assessment of their level of maturity by assessing their NCSS objectives. This will help them to enhance and build cybersecurity capabilities at both the strategic and the operational levels.

On a more practical level, ENISA identified various benefits of the NCAF, namely that it:



1.6 Principles of the framework

The NCAF presented in this section is based on the needs highlighted by the Member States and built around the following set of requirements.



The self-assessment framework is designed to support Member States in strengthening their cybersecurity capabilities by defining maturity levels at multiple layers – objective level, cluster level and overall (global) level.

1.7 Other Usages

It needs to be noted that the NCAF may also be used as a basis for the discussion within the voluntary peer reviews as set out by Article 19 of the NIS2 Directive. In this context, the NCAF can be used as a tool to support mutual learning and exchange of national practices.

The EU-CSI also uses some of the NCAF's questions to measure certain aspects of a country's cybersecurity posture. The EU-CSI might evolve in closer alignment with the NCAF.

SECTION 2

NCAF methodology

2. National capabilities assessment framework methodology

The **main objective** of the NCAF is to measure the maturity level of **Member States' cybersecurity capabilities**, supporting them in evaluating their national cybersecurity posture, increasing awareness of their maturity level, identifying areas for improvement and building cybersecurity capabilities.

2.1 Maturity levels

The maturity model retains the **five-level structure** introduced in the NCAF of 2020. These levels align with the successive stages through which Member States progress when developing cybersecurity capabilities in relation to each NCSS objective. They represent a continuum of increasing maturity, beginning with the foundation **level 1** – at which Member States have taken initial steps, having established broad goals and implemented the minimum measures to build cybersecurity capabilities in the areas covered by the NCSS objectives – and progress up to advanced **level 5**, at which the strategy for cybersecurity capacity building is dynamic and responsive to evolving environmental developments.

IMPORTANT NOTICE: Level 5 is considered as extremely high and very few countries, if any, are expected to reach this level for all objectives. Still, it is important to include such a level to illustrate the horizon that a country may aspire to.

Table 1 presents the maturity levels developed for NCAF 2.0.

Table 1: The ENISA National Capabilities Assessment Framework five-level maturity scale

Level 1 – Foundation	Level 2 – Developing	Level 3 – Established	Level 4 – Mature	Level 5 – Advanced
The Member State (MS) has adopted an NCSS. However, a comprehensive and structured approach to capacity-building across all NCSS objectives is still lacking. Initial steps may include broad goals and limited measures or initiatives, which are often generic and not systematically implemented.	A national approach to capacity building aligned with NCSS objectives has been decided on. Action plans and activities are in place, although many are in the early stages of implementation. Some measures are being planned and initiated in priority areas. Key stakeholders have been identified and are beginning to	Capacity-building measures and initiatives are systematically developed and implemented across the NCSS objectives. Governance structures for implementation and oversight are fully operational, with clearly assigned responsibilities. Activities are executed with allocated resources, specified timelines and consistent	Cybersecurity planning and implementation are strategically aligned across sectors and levels of governance. The national action plan is prioritised, optimised and supported by long-term, institutionalised mechanisms (e.g., legislation, funding, national agencies). Capacity-building activities are regularly evaluated and refined based on performance	The Member State demonstrates a dynamic and adaptive strategy, attentive to evolving technological, geopolitical and threat landscapes. A culture of innovation is fostered through ongoing research and international cooperation. Strategic decisions are driven by continuous monitoring of emerging challenges and

	engage in the process.	documentation at the national level. Relevant stakeholders are regularly engaged throughout the policy cycle. The Member State contributes to selected EU-level initiatives based on its priorities.	data. Formal, cross-sectoral collaboration mechanisms and structured cooperation with other Member States are in place. Monitoring, performance assessment and continuous improvement mechanisms are embedded to identify gaps and success factors, and guide evidence-based decision-making.	forward planning, enabling timely and effective responses

2.2 Strategic objectives identified within european national cybersecurity strategies

Despite the diversity of the NCSSs and action plans, Member States often establish strategic objectives that cluster around similar themes. ENISA has therefore analysed these common objectives and compiled the following list of 20 key strategic objectives [14]. This list not only builds on the 17 objectives included in the original NCAF but also introduces new thematic areas:

- strengthen the cyber resilience and cyber hygiene of the private sector, including small and medium-sized enterprises (SMEs);
- promote cybersecurity awareness and cyber hygiene on cybersecurity;
- address the cybersecurity skills gap;
- foster research and development (R & D) and innovation;
- enhance incident preparedness and response (IPR);
- address cybercrime;
- engage in international cooperation;
- establish trusted information-sharing mechanisms;
- establish mutual assistance processes;
- develop crisis-management frameworks;
- secure digital identity and build trust in digital public services;
- establish national-level risk assessment;
- strengthen national cybersecurity governance;

[14] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/objectives?objective=1.

- establish cybersecurity risk-management measures;
- establish incident-reporting mechanisms;
- balance security with privacy;
- improve the cybersecurity of the supply chain;
- protect critical sectors;
- establish a coordinated vulnerability disclosure (CVD) policy;
- promote active cyber protection (ACP).

2.3 Goals of the strategic objectives

The 20 key strategic objectives were thoroughly examined, leading to the development of a set of goals for each objective. These goals represent the core characteristics of each objective and provided guidance for the formulation of the corresponding maturity questions. Table 2 presents the goals associated with each objective.

Table 2: Common strategic objectives covered by Member States in their NCSSs

OBJECTIVE NUMBER	NCSS STRATEGIC OBJECTIVE	GOALS
1	Strengthen the cyber resilience and cyber hygiene of the private sector, including SMEs	▶ Enforce mandatory cybersecurity standards by law to ensure that businesses implement appropriate security measures. ▶ Promote and develop cybersecurity education, training, awareness and R & D initiatives to foster a strong security culture across the private sector. ▶ Provide practical guidance and promote good cyber-hygiene practices tailored to the operational needs of businesses, particularly SMEs. ▶ Provide guidance and assistance in strengthening the resilience of SMEs (e.g., vouchers, support programmes). ▶ Strengthen the cyber-hygiene baseline of SMEs.
2	Promote cybersecurity awareness and cyber hygiene on cybersecurity	▶ Develop and implement ongoing awareness-raising initiatives to educate civil society and academia about cybersecurity threats. ▶ Offer guidance on good cyber-hygiene practices and controls to users and entities. ▶ Include the need for cybersecurity awareness and cyber hygiene in the NCSS.
3	Address the cybersecurity skills gap	▶ Integrate the promotion and development of education and training on cybersecurity and cybersecurity skills development into the NCSS. ▶ Enhance the development of cybersecurity skills in technical, operational and strategic areas. ▶ Adopt specific measures within the NCSS to mitigate the cybersecurity skills shortage and close skills gaps.

		▶ Undertake EU-wide collaborative initiatives to promote the single market for cybersecurity skills.
4	Foster R & D and innovation	▶ Support R & D initiatives to create and enhance innovative cybersecurity tools and secure network infrastructure. ▶ Encourage the integration of innovative technologies (e.g. AI and post-quantum cryptography) in cybersecurity solutions to enhance detection and prevention capabilities. ▶ Promote R & D activities within the NCSS that facilitate the use of automated or semi-automated tools in cybersecurity and support the sharing of data necessary for technology advancement. ▶ Ensure that the use of cutting-edge technologies complies with EU data protection law. ▶ Exploit the requirements of data protection by design and by default. ▶ Encourage participation in EU and global innovation networks.
5	Enhance IPR	▶ Develop and implement comprehensive frameworks and protocols for IPR and acknowledge their existence in the NCSS. ▶ Enhance the role of national/governmental computer security incident response teams (CSIRTs) as central coordinating bodies, ensuring effective collaboration among public and private sector stakeholders. ▶ Integrate IPR activities such as incident handling, reporting, analysis and response coordination at the national and international levels. ▶ Develop measures to ensure preparedness, responsiveness and recovery from incidents, focusing on cooperation between private and public sectors.
6	Address cybercrime	▶ Establish and coordinate efforts of relevant stakeholders to fight cybercrime collaboratively. ▶ Encourage awareness raising about identification of cybercriminal activities among essential and important entities. ▶ Participate in coordination efforts among competent authorities and law enforcement facilitated by the European Cybercrime Centre (EC3) and ENISA. ▶ Strengthen the detection, investigation and prosecution capabilities of law enforcement and judicial authorities.

7	Engage in international cooperation	▶ Establish and maintain international cybersecurity partnerships to support joint actions and strategic alignment on cybersecurity. ▶ Promote cross-border incident response coordination through trusted international channels and protocols. ▶ Participate in information-sharing mechanisms internationally to better comprehend the latest developments of the threat landscape. ▶ Support CSIRTs' participation in international cooperation networks and their coordination protocols. ▶ Promote responsible state behaviour in cyberspace and support coordinated EU responses to malicious cyber activities (the EU cyber diplomacy toolbox and the strategic compass). ▶ Defend a global, open, secure and interoperable internet and strengthen international cooperation through multilateral and multistakeholder engagement (e.g., the cyberdefence policy, the cybersecurity strategy for the Digital Decade, the European External Action Service (EEAS) cyber dialogue and engagement in international cyber dialogues and forums such as those of the UN, the Organization for Security and Co-operation in Europe (OSCE), NATO and the Global Forum on Cyber Expertise (GFCE)).
8	Establish trusted information-sharing mechanisms	▶ Integrate robust, trusted information-sharing cooperation between public and private stakeholders within the NCSS. ▶ Foster strategic partnerships between critical-infrastructure owners and public authorities on information exchange about threats, vulnerabilities and national security status to enhance situational awareness. ▶ Support information-sharing and analysis centres (ISACs) and public–private partnerships (PPPs) as strategic tools for pooling expertise and resources. ▶ Implement procedures and tools that facilitate voluntary cybersecurity information sharing. ▶ Address legal, organisational and cultural barriers to information sharing.
9	Establish mutual assistance processes	▶ Establish mutual assistance processes among Member States to ensure effective cooperation and support in supervisory and enforcement actions across borders. ▶ Develop frameworks for information sharing, inspections and audits among Member States' authorities. ▶ Promote coordination and consultation among Member States' authorities to address potential refusal of assistance. ▶ Encourage joint supervisory action through mutual agreement.
10	Develop crisis-management frameworks	▶ Develop a comprehensive cyber crisis-management framework whose concept and measures are anchored within the NCSS, ensuring coherence with general national crisis-management structures. ▶ Establish dedicated cyber crisis-management authorities and empower them with adequate resources to manage large-scale cybersecurity crises.

		▶ Enhance cross-border cooperation and coordination in cyber crisis response by implementing transboundary collaboration mechanisms within the cyber crisis-management framework. ▶ Embed regular testing of the crisis-management framework in the NCSS.
11	Secure digital identity and build trust in digital public services	▶ Promote the digital transformation of public administrations with a focus on ensuring cybersecurity, efficiency and accessibility of digital public services. ▶ Build trust in government in relation to digital identity and public services.
12	Establish national-level risk assessment	▶ Establish a mechanism to consolidate risk assessments across sectors, ensuring a national-level view of critical assets and threats, in line with existing requirements under NIS2 and the Critical Entities Resilience Directive (CER Directive). ▶ Align cybersecurity strategy objectives with national security needs through comprehensive national risk assessment. ▶ Facilitate sector-specific risk assessments to address the risks to critical sectors.
13	Strengthen national cybersecurity governance	▶ Create a governance framework to achieve the objectives and priorities set out in the NCSS and related policies, including on critical sectors. ▶ Establish the roles, responsibilities and accountability of relevant stakeholders and create a list of the stakeholders and authorities. ▶ Establish and maintain cooperation and the coordination of activities related to the implementation of the NCSS at the national level, especially between the competent authorities, CSIRTs and single points of contact designated under NIS2, including cross-sectoral and cross-border collaboration. ▶ Enhance coordination among competent authorities under NIS2 for the purpose of information sharing and carrying out an assessment at the level of capabilities (including financial, technical and human resources) and the effectiveness of the performance of their operational and supervisory tasks.
14	Establish cybersecurity risk-management measures	▶ Establish a framework that promotes and facilitates the implementation of suitable risk-management measures by essential and important entities to protect the security of their systems. ▶ Establish mechanisms to promote and facilitate the adoption of relevant technologies and their incorporation into state-of-the-art risk-management measures demonstrating commitment to innovation and technological capacity building.
15	Establish incident-reporting mechanisms	▶ Establish incident-reporting mechanisms for essential and important entities to ensure the timely reporting of significant incidents to the CSIRTs or competent authorities in accordance with NIS2. ▶ Encourage essential and important entities to notify their service users about incidents that are likely to affect service delivery. ▶ Require essential and important entities to provide adequate information to CSIRTs or competent authorities to assess the potential cross-border impact of incidents.

		▶ Ensure seamless communication and rapid notification processes between competent authorities and CSIRTs. ▶ Develop protocols for timely information sharing with single points of contact in cases of cross-border or cross-sector incidents.
16	Balance security with privacy	▶ Embed the principles of security and privacy in the NCSS, seeking balance between them both. ▶ Contribute to enhancing the protection of the right of privacy within cybersecurity. ▶ Foster cooperation between data protection authorities, national competent authorities and other stakeholders.
17	Improve the cybersecurity of the supply chain	▶ Implement state-of-the-art measures to address the cybersecurity of the supply chain for ICT products and ICT services used by essential and important entities for the provision of their services. ▶ Introduce measures (including awareness raising and sharing best practices) aimed at strengthening the cyber resilience of SMEs, in particular in relation to their supply chain. ▶ Conduct coordinated security risk assessments of critical supply chains as specified in NIS2. ▶ Set baseline security requirements. ▶ Establish policies and provide guidelines to ensure that public administration procurement procedures include clear cybersecurity requirements and prioritise the selection of trustworthy and reliable suppliers.
18	Protect critical sectors	▶ Ensure strategic alignment between the protection of critical sectors (as per Annexes I and II to NIS2) and related physical resilience obligations under the CER Directive. ▶ Adopt specific policies to ensure the availability, integrity and confidentiality of critical sectors, including the public core of the internet and underseas communications cables, if applicable.
19	Establish a CVD policy	▶ Establish a CVD process outlining a structured approach for reporting vulnerabilities to manufacturers and service providers. ▶ Develop and implement a national policy to facilitate CVD and provide a framework for managing vulnerability reports. ▶ Promote the adoption of protective guidelines and legal clarity to foster good-faith vulnerability research, including, where appropriate, exemptions or safeguards from civil or criminal liability, in line with national legal frameworks.
20	Promote ACP [15]	▶ Integrate ACP into the NCSS. ▶ Promote policies on proactive ACP measures as part of a wider defence strategy. ▶ Promote the implementation of internal (and, in the best case scenario, external) ACP capabilities to prevent, detect, monitor and mitigate network security breaches. ▶ Promote the use of ACP tools and services to enhance the ability to share threat intelligence.

[15] For the definition of ACP, please refer to recital 57 of NIS2.

2.4 Clustering of the objectives

NCAF 2.0 is structured around **four clusters**, each representing a key thematic area of cybersecurity capacity within an NCSS: (1) capacity building and awareness, (2) cooperation and collaboration, (3) cybersecurity governance and (4) regulatory and policy frameworks.

1) **Capacity-building and awareness**: This cluster assesses the capacity of Member States to raise awareness of cybersecurity risks and threats and to strengthen cyber resilience and cyber hygiene. It also evaluates their ability to continuously develop cybersecurity capabilities and enhance the overall level of knowledge and skills within this domain. Furthermore, it addresses improvements in IPR and advancements in cybersecurity R&D.

2) **Cooperation and collaboration**: This cluster evaluates cooperation and information sharing between different stakeholders at both the national and the international levels (including as part of mutual assistance processes), recognising it as an important tool for better understanding and responding to a constantly changing threat environment. It also assesses the capacity of Member States to address and counter cybercriminal activities.

3) **Cybersecurity governance**: This cluster measures the capacity of Member States to establish effective governance and good practices in the cybersecurity domain. It considers various aspects of national cybersecurity governance, risk assessment and management, while supporting the development of crisis-management and incident-reporting mechanisms and fostering trust in public services and digital identities.

4) **Regulatory and policy frameworks**: This cluster measures the capacity of Member States to establish the necessary regulatory and policy instruments to improve supply chain cybersecurity, promote ACP and safeguard critical information infrastructure. It also assesses their capacity to create a policy framework for CVD or a regulatory framework that balances security with privacy.

Depending on its focus, each cluster includes a set of strategic objectives that Member States may incorporate into their NCSS. While clustering is an integral feature of NCAF 2.0, Member States are free to organise the objectives in their NCSS as they see fit. The four clusters and underlying objectives of NCAF 2.0 are structured as follows.

Cluster #1: Capacity-building and awareness

1) Strengthen the cyber-resilience and hygiene of private sector, including SMEs.
2) Promote cybersecurity awareness and cyber hygiene on cybersecurity.
3) Address the cybersecurity skills gap.
4) Foster R&D and innovation.
5) Enhance IPR.

Cluster #2: Cooperation and collaboration

6) Address cybercrime.
7) Engage in international cooperation.

8) Establish trusted information-sharing mechanisms.
9) Establish mutual assistance processes.

Cluster #3: Cybersecurity governance

10) Develop crisis management frameworks.
11) Secure digital identity and build trust in digital public services.
12) Establish national level risk assessment.
13) Strengthen national cybersecurity governance.
14) Establish cybersecurity risk-management measures.
15) Establish incident reporting mechanisms.

Cluster #4: Regulatory and policy frameworks

16) Balance security with privacy.
17) Improve the cybersecurity of the supply chain.
18) Protect critical sectors.
19) Establish a CVD policy.
20) Promote ACP.

2.5 Scoring mechanism

The **scoring mechanism** of the framework takes into consideration the elements outlined above and the principles listed in Section 1.6. The model generates a score based on two parameters: the **maturity level** and the **coverage ratio**. Each parameter can be calculated at one of three different levels: (1) per objective, (2) per cluster of objectives or (3) overall.

Scores at the objective level

The **maturity level score** provides an overview of a Member State's maturity by showing which capabilities and practices were put in place. The maturity score is calculated as the highest level for which the respondent has satisfied all of the requisites (i.e. answered 'yes' to all of the requisite questions), including all requisites of the previous maturity levels.

The **coverage ratio** indicates the extent to which all indicators for an objective are answered positively, irrespective of their maturity level. It complements the maturity level score by considering all indicators measuring the objective. The coverage ratio is calculated as the proportion of questions for which the answer is positive relative to the total number of questions within the objective.

It is important to note that, throughout this document, the term **'score'** refers collectively to both the maturity level and the coverage ratio. Figure 1 shows the scoring mechanism per objective.

Figure 1: Scoring mechanism per objective

Additionally, to account for the specific characteristics of each Member State while also ensuring a consistent overall perspective, the score is calculated from two different samples at the cluster and overall levels:

- **General scores**: based on a complete sample that includes all objectives within the cluster or within the overall framework (from one to 20);

- **Specific scores**: based on a tailored sample that covers only the objectives selected by the Member State (usually corresponding to the objectives present in the country's NCSS) 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 maturity levels of all objectives within that cluster.

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

For example, as shown in Section 2.4, cluster 1, 'Capacity building and awareness', is composed of five objectives. Assuming that the respondent chose to assess only the first three objectives, but not the fourth and fifth, and assuming that the first three objectives present levels of maturity of 2, 4 and 4, then the level of maturity of the cluster considering all the objectives is level 2 (cluster 1 generic maturity level = (2 + 4 + 4) / 5), while the level of maturity of the cluster considering only the specific objectives selected by the assessor is level 3 (cluster 1 specific maturity level = (2 + 4 + 4) / 3).

The **general coverage ratio of each cluster** is calculated as the proportion of positively answered questions to the total number of questions within the cluster.

The **specific coverage ratio of each cluster** is calculated as the proportion of positively answered questions to the total number of questions within the cluster that pertain to the objectives selected by the Member State (usually corresponding to the objectives present in the NCSS of the specific country).

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 1 to 20.

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 has chosen 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 of positively answered questions to the total number of questions across the objectives in the framework (from 1 to 20).

The **overall specific coverage ratio of a country** is calculated as the proportion of positively answered questions to the total number of questions within the objectives that the Member State has

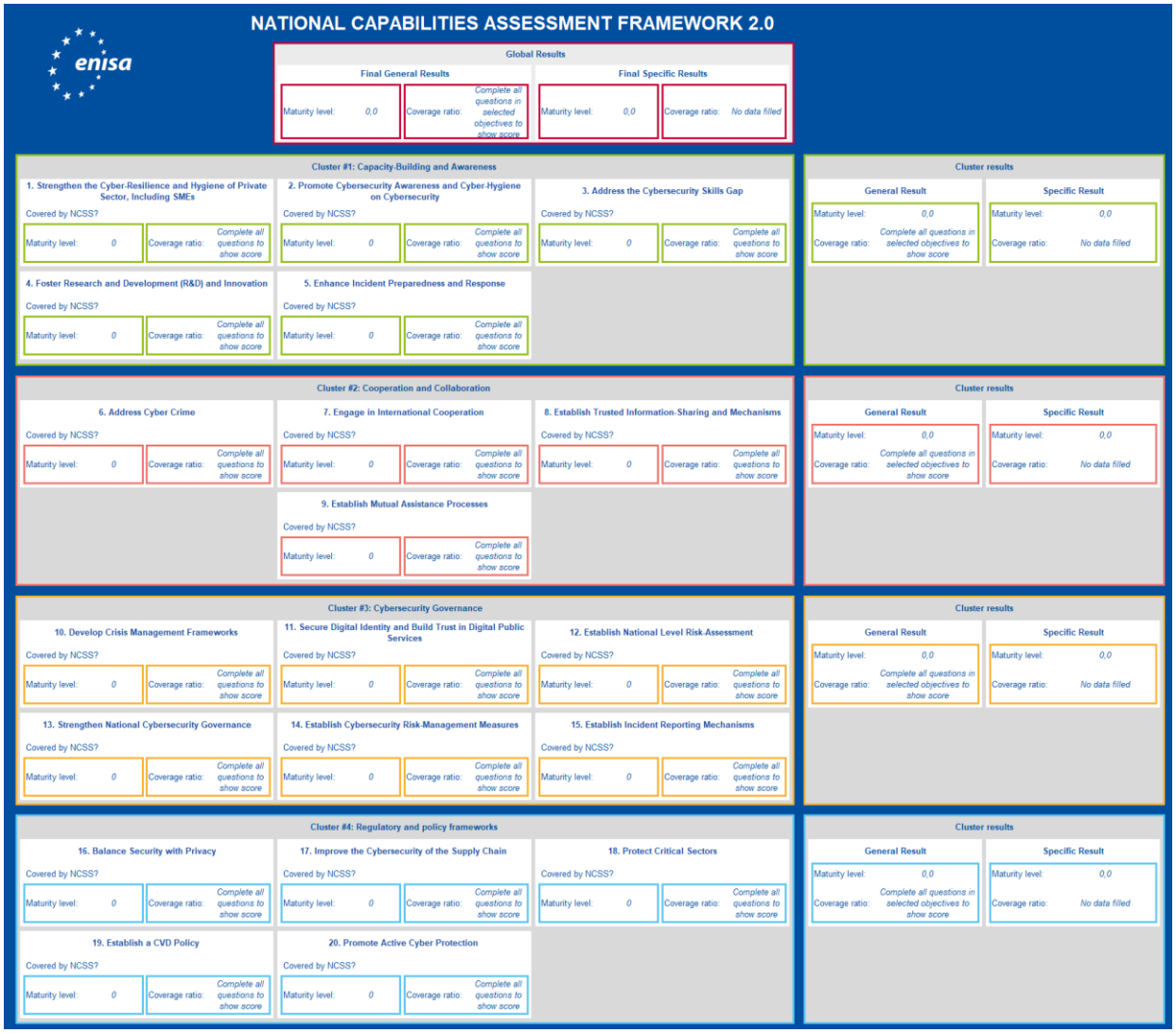
chosen to assess (usually corresponding to the objectives present in the NCSS of the specific country).

For each indicator, respondents may also select a third option, ‘don’t know / not applicable’. When selected, the indicator is excluded from the total calculation of the results. Figure 2 shows the overall scoring mechanism.

The maturity levels at the cluster level and at the overall level are calculated using the arithmetic mean to show the progress between two assessments. The alternative approach of determining the cluster and overall maturity levels based on the least mature objective, while valid from a maturity standpoint, does not capture the progress made in areas covered by other objectives.

Because the cluster and overall levels are consolidated for reporting purposes, the arithmetic mean has been selected as the calculation method. However, for more precise insights, reporting should be based on the scores at the objective level.

Figure 2: Overall scoring mechanism



SECTION 3

NCAF indicators

3. National capabilities assessment framework indicators

This section presents the ENISA NCAF indicators. The following sections are organised by cluster.

For each cluster, a table presents the full set of indicators in the form of questions aligned with specific maturity levels. The questionnaire serves as the primary instrument for the self-assessment. For each objective, there are two sets of indicators included:

- **generic strategy maturity questions** – five generic questions for each maturity level and repeated across all objectives;
- **cybersecurity capacity questions** – 871 cybersecurity capacity questions, numbered for each maturity level and specific to the area covered by the objective.

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

Each question is assigned an identification number composed of the:

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

For example, question 14.2.5 refers to the fifth question in maturity level 2 of strategic objective 14: 'Establish cybersecurity risk-management measures'.

Unless otherwise specified, all questions apply at the national level. The pronoun 'you' refers to the Member State in a general sense, not to the individual or government body conducting the assessment.

The list of objectives and their corresponding goals is provided in Section 2.3.

3.1.1 Cluster #1: Capacity-building and awareness

1. Strengthen the Cyber-Resilience and Hygiene of Private Sector, Including SMEs

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
1 – Strengthen the cyber-resilience and hygiene of private sector, including Small and Medium Enterprises (SMEs)	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Do you promote the use of European and international standards and technical specifications for securing network and information systems?	1	Have you considered mandating the implementation of European, national and international cybersecurity standards and frameworks (e.g. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) standard ISO/IEC 27001, the National Institute of Standards and Technology (NIST) framework, the CyberFundamentals framework), especially for ICT products,	1	Is there a mandatory national cybersecurity standard applicable to essential and important entities, aligned with NIS2 requirements and incorporating European and international best practices?	1	Are mandatory standards reviewed regularly, coordinated across sectors and aligned with EU-level frameworks (e.g. the CRA, the EU cloud services scheme) to ensure interoperability and continuous improvement, while avoiding discrimination against specific technologies?	1	Is there a process in place to maintain and update national cybersecurity standards in line with EU regulatory developments, emerging threats and international revisions (e.g. the transition to the latest version of ISO/IEC 27001)?	1

				services and processes through EU certification schemes, for essential and important entities?						
	2	Have key priorities for cybersecurity awareness-raising and cyber-hygiene initiatives for private sector entities, including SMEs, been identified?	1	Have you developed or supported national cybersecurity awareness-raising and training programmes aimed at private sector entities, aligned with NIS2 and the European cybersecurity skills framework (ECSF)?	1	Are national cybersecurity training programmes operational, with dedicated funding, stakeholder involvement and measurable outcomes (aligned with the digital Europe programme priorities)?	1	Do you involve the private sector, in any form, in cybersecurity awareness-raising and training initiatives (e.g. course design and delivery, internships, work placements or facilitation of free training offered by the Cybersecurity Skills Academy's pledgers, such as ISC2 (the International Information System Security Certification Consortium), the SANS (SysAdmin, Audit, Network and Security) Institute and the ISACA (Information Systems Audit and Control Association))?	1	Do you continuously monitor developments in technological trends and evolving threats, and integrate them into cybersecurity awareness-raising and training programmes for private sector entities, incorporating lessons learned from incidents and research outputs?	1
	3	Does your NCSS identify the need to provide guidance and awareness-raising activities, including ad hoc initiatives (e.g. capture-the-flag exercises, webinars or workshops), to enhance cyber resilience and promote cyber-hygiene best practices in the private sector?	1	Do you have a designated budget to launch best practice awareness-raising campaigns and structured guidance on cyber hygiene and cyber resilience for private sector entities?	1	Is cyber-hygiene guidance included in private sector policies and reinforced by national awareness campaigns or recognition schemes in partnership with industry associations?	1	Do you have a mechanism to identify and assess the most effective approaches for digital outreach to private sector entities, including coordinated cross-sector campaigns and incentive programmes linked to EU-wide events?	1	Do you have mechanisms to ensure that awareness-raising campaigns and cyber-hygiene practices for essential and important entities remain relevant to technological advancements, evolving threats and regulatory changes, and lead to observable behavioural changes?	1
	4	Have you identified the specific cybersecurity	1	Are cybersecurity guidance materials or	1	When developing cybersecurity materials	1	Do you gather feedback from SMEs that are	1	Do you adapt cybersecurity guidance	1

		needs for SMEs excluded from the scope of NIS2, to enhance their resilience as well?		toolkits also available for SMEs that are excluded from the scope of NIS2, to support basic cyber hygiene and cyber resilience?		and toolkits and/or guidelines for SMEs that are excluded from the scope of NIS2, do you emphasise simplicity and actionable guidance in line with EU frameworks, ENISA recommendations and/or SME-specific needs?		excluded from NIS2, to improve the usability and relevance of cybersecurity toolkits and guidance materials?		and toolkits based on SME characteristics, the evolving threat industry context, ICT dependency and the criticality of processed information?	
	5	Have you nominated a national coordination centre (NCC) and established basic communication channels to inform SMEs about their role and the potential benefits of participating in initiatives supported by the European Cybersecurity Competence Centre (ECCC)?	1	Does the NCC engage with SMEs and sector associations to raise awareness of available EU-level resources (e.g. ECCC funding calls such as the digital Europe programme and Horizon Europe, training materials and research outputs)?	1	Does the NCC facilitate access for SMEs to ECCC resources, EU funding opportunities and research outputs, supporting their adoption of advanced cybersecurity solutions?	1	Is there a structured NCC programme that uses ECCC-supported initiatives (e.g. targeted training, threat intelligence sharing) to improve SMEs' cyber resilience and cyber hygiene, including the adoption of privacy-by-design security technologies?	1	Have the NCC, the ECCC and national stakeholders cooperated on designing a mechanism to assess and refine SME-focused cybersecurity programmes, taking into account feedback, emerging threats and innovations?	1
	6	Do you invite industry associations and SMEs to participate jointly in any formal or informal cybersecurity awareness-raising events or platforms?	1	Is there a national programme or initiative dedicated to supporting cooperation between industry associations and SMEs, such as through scale training or shared resources?	1	Do you encourage industry associations and SMEs to be part of a national or sectoral information systems audit and control association, to strengthen cyber-threat awareness and incident response capabilities?	1	Do you assess the effectiveness of cooperation between industry associations and SMEs (e.g. using associations as trusted multipliers for cybersecurity outreach) and, more broadly, the impact of joint initiatives on SMEs' preparedness (e.g. national- or EU-level exercises), based on measurable outcomes and feedback?	1	Do you actively encourage industry associations and SMEs to participate in international- and EU-level support networks (e.g. the ECCC, Global Cyber Alliance) to discuss forward-looking information on threats and cyber resilience?	1

2. Promote Cybersecurity Awareness and cyber-hygiene on cybersecurity

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
2 – Promote cybersecurity awareness and cyber hygiene on cybersecurity	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Is the need to raise awareness of cybersecurity and privacy issues among citizens and entities explicitly addressed in your NCSS?	1	Has a single point of contact been designated to coordinate and assist in cybersecurity awareness-raising activities at the national or regional levels?	1	Have you developed a national cybersecurity awareness framework to guide the building of awareness at the national level?	1	Are providers of services (e.g. telecommunications, banking, digital platforms) incentivised to invest in cybersecurity awareness and cyber hygiene?	1	Is there a process in place to regularly update your national cybersecurity awareness framework to ensure that it remains relevant to the evolving national cybersecurity threat landscape?	1
	2	Have key priorities for national cybersecurity awareness-raising and cyber-hygiene initiatives been identified?	1	Have you identified specific target audiences for users' cybersecurity awareness-raising and cyber-hygiene activities (e.g. citizens, young people, older people, public sector employees, personnel of SMEs, employees of essential and important entities)?	1	Have you developed a communication plan/strategy for cybersecurity awareness-raising campaigns and cyber-hygiene activities and initiatives for the targeted audiences?	1	Do you evaluate your cybersecurity awareness-raising and cyber hygiene activities after execution?	1	Are changes in the national cybersecurity threat landscape reflected in your cybersecurity awareness-raising and cyber-hygiene initiatives to ensure that they continue providing timely and effective information?	1
	3	Have you assessed the effectiveness of different delivery methods for cybersecurity awareness-	1	Do you use different delivery methods for cybersecurity awareness-raising	1	Are different delivery methods systematically employed during cybersecurity	1	Do you have any mechanisms in place to identify the most relevant media or communication	1	Are new delivery methods regularly explored or developed to enhance the	1

		raising campaigns (e.g. social media, public service announcements, community events)?		campaigns, at least on an ad hoc basis?		awareness-raising and cyber-hygiene activities to maximise effectiveness?		channel depending on the target audience to maximise outreach and engagement?		effectiveness of cybersecurity awareness-raising and cyber-hygiene campaigns?	
	4	Are there any formal or informal coordination actions between cybersecurity and legal/policy teams to share information used to drive awareness-raising and cyber-hygiene activities?	1	Have mechanisms been proposed or initiated to identify relevant external and internal factors (e.g. threat intelligence, policy updates, legal changes) that could be used to enhance cybersecurity awareness-raising and cyber-hygiene efforts?	1	Do you have any mechanisms in place to identify target areas for cybersecurity awareness-raising measures based on cybersecurity intelligence sources (e.g. the ENISA Threat Landscape report, information on the national and international threat landscapes, feedback from national cybercrime centres)?	1	Are your cybersecurity awareness-raising and cyber-hygiene activities updated (frequently or on an ad hoc basis) to reflect internal and external factors (e.g., recent security incidents or updated policies or legislation)?	1	Are mechanisms in place to ensure that cybersecurity awareness-raising measures remain continuously relevant, reflecting technological developments, changes in the national and international threat landscape, applicable legal and regulatory requirements, and national cybersecurity directives?	1
	5	Does your NCSS or other strategic document acknowledge the need to tailor cybersecurity awareness-raising and cyber-hygiene material to different user groups (e.g. individuals, SMEs, healthcare providers, educators)?	1	Are tailored materials and recommendations developed for specific user groups (e.g. individuals, SMEs, healthcare providers, educators) on basic cyber-hygiene practices?	1	Do you bring together stakeholders with experts (e.g. relevant associations and community groups) and communication teams to tailor the content of cybersecurity awareness-raising and cyber-hygiene campaigns?	1	Do you consult with behavioural experts to tailor your cybersecurity awareness-raising and cyber-hygiene campaigns to the target audience?	1	Are the materials provided regularly reviewed and updated to reflect the evolving national cybersecurity threat landscape and threats specific to target sectors or communities?	1
	6	Is there a plan to establish a set of minimum expected cybersecurity practices (e.g. multifactor authentication, secure passwords) and tools that can be adopted by citizens and SMEs?	1	Have minimum expected cybersecurity practices been established, supported by tools developed to help citizens and SMEs adopt secure behaviours online?	1	Are the minimum expected cybersecurity practices and tools actively promoted among citizens and SMEs to increase their adoption in a structured and coordinated manner?	1	Do you regularly review and update the minimum expected cybersecurity practices and tools to ensure that they provide appropriate protection against current and emerging threats?	1	Are minimum expected cybersecurity practices and tools updated based on foresight research and predictive techniques to prepare citizens and SMEs for emerging and future cybersecurity threats?	1

	7	Does your leadership publicly support the need to train educators, communicators, human resources (HR) professionals and local authorities to effectively convey cyber awareness-raising and cyber-hygiene messages?	1	Are resources available for educators, communicators, HR professionals and local authorities to support them in effectively delivering cybersecurity awareness-raising and cyber-hygiene activities?	1	Is training provided to educators, communicators, HR professionals and local authorities to enable them to effectively deliver cybersecurity awareness-raising and cyber-hygiene messages?	1	Is there a mechanism in place to evaluate whether the dedicated resources and training provided to educators, communicators, HR professionals and local authorities on delivering cybersecurity awareness-raising and cyber-hygiene messages are allocated efficiently and provide adequate support?	1	Are relevant educators, communicators, HR professionals and local authorities encouraged to continuously enhance their delivery skills by integrating innovative methods and emerging best practices into cybersecurity awareness-raising training?	1
	8	Do you have policies in place recognising the need to focus on cybersecurity awareness raising and cyber hygiene for hard-to-reach or digitally excluded communities?	1	Have you developed any cybersecurity awareness-raising or cyber-hygiene initiatives targeting hard-to-reach or digitally excluded communities?	1	Is there structured collaboration with civil society, digital influencers, consumer organisations or local governments in developing and distributing cybersecurity awareness-raising or cyber-hygiene content for hard-to-reach or digitally excluded communities?	1	Are statistics on cybersecurity literacy among hard-to-reach or digitally excluded communities regularly collected and evaluated to optimise awareness-raising and cyber-hygiene programmes and to identify new channels for outreach?	1	Are innovative communication channels actively explored to distribute key awareness-raising and cyber-hygiene messages to hard-to-reach or digitally excluded communities?	1
	9	Is the need to establish national metrics (e.g. surveys, incident trends, phishing test results) to track awareness levels, cyber-hygiene behaviours and programme effectiveness identified in your cybersecurity policies or strategy documents?	1	Has any national survey been conducted to measure cybersecurity awareness levels and cyber-hygiene behaviours among citizens and entities?	1	Have national metrics such as surveys, incident trends or phishing test results been established to monitor cybersecurity awareness levels and cyber-hygiene behaviours among citizens and entities?	1	Do you perform periodic evaluations to measure attitude shifts or behaviour changes regarding cybersecurity and privacy matters among citizens and entities?	1	Are real-time data leveraged to evaluate trends in the national cybersecurity landscape and identify topics for ad hoc awareness-raising measures addressing emerging threats?	1
	10	Do national strategies or policies consider the integration of cybersecurity into digital	1	Do you encourage primary, secondary and tertiary education institutions to integrate	1	Are primary, secondary and tertiary education institutions provided with supporting materials to	1	Are statistics on cybersecurity literacy among children and students regularly	1	Are topics related to disruptive technologies incorporated into cybersecurity curricula	1

		literacy and civics curricula from primary to tertiary education as part of awareness-raising and cyber-hygiene initiatives?		cybersecurity into digital literacy and civics curricula?		include cybersecurity in their digital literacy and civics curricula?		collected and evaluated to optimise awareness-raising and cyber-hygiene materials and recommendations for each level of education?		to prepare younger generations for emerging and future threats?	
	11	Is there a plan to establish a national cybersecurity portal that provides information, materials and toolkits to support personal and organisational cyber hygiene as part of awareness-raising measures?	1	Do you have resources that are easily available and identifiable (e.g. through a single online portal or in an awareness kit) for users and entities seeking to educate themselves on cyber-hygiene topics?	1	Do you have a national cybersecurity portal that actively provides cyber-hygiene-related information, materials and toolkits for stakeholders of varying types and maturity levels (e.g. citizens, SMEs, public administration entities)?	1	Do you regularly collect and utilise user feedback to update materials and resources on cyber hygiene that are available through your national cybersecurity portal to reflect the latest cybersecurity trends and needs?	1	Does your national cybersecurity portal include interactive, dynamic content and continuously updated information (e.g. a chatbot, gamification, live broadcasts, daily/weekly cybersecurity-related news) to enhance user engagement and broaden reach?	1

3. Address the Cybersecurity Skills Gap

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
3 – Address the cybersecurity skills gap	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have you considered implementing a coordinated national strategy with clear objectives and measurable outcomes to address shortages in cybersecurity specialists?	1	Have you identified the key national stakeholders who can contribute to developing cybersecurity specialists' competencies?	1	Have you adopted a national roadmap with concrete steps and designated stakeholders to build cybersecurity specialists' professional capabilities?	1	Are mechanisms in place to regularly assess and update the national cybersecurity roadmap in line with the evolving needs of cybersecurity specialists?	1	Do you monitor emerging technical, legal, and socio-economic risks and trends among cybersecurity specialists, and adapt your national roadmap accordingly?	1
	2	Is the cybersecurity skills gap explicitly included in your NCSS or related policy documents?	1	Have you established a methodology to assess cybersecurity skills at the national level?	1	Have you conducted a national assessment of cybersecurity skills across technical, legal, and policy domains, including the public and private sectors, and academia?	1	Do you regularly conduct national assessments of cybersecurity skills to update and adapt your national roadmap to address the cybersecurity skills gap?	1	Have you conducted or planned structured foresight exercises to identify emerging trends and future needs in the national cybersecurity workforce?	1
	3	Have you conducted a study on the integration of cybersecurity fundamentals into national educational curricula?	1	Do you provide training for educators, regardless of their field, on information security and privacy issues such as online safety, personal	1	Does the national education policy promote cybersecurity awareness and internet safety courses at early stages of education, including primary,	1	Do you promote information security courses in secondary and tertiary education for students beyond computer science, including courses tailored	1	Do you regularly monitor cybersecurity trends and provide tailored guidance on cybersecurity education across all levels of the	1

				data protection and cyberbullying?		middle, and high school?		to other professional fields?		national education system?	
	4	Does your current or upcoming NCSS include measures to promote and develop cybersecurity education, training and skills for citizens and relevant stakeholders through dedicated programmes?	1	Have strategic objectives and key policy measures been established to promote cybersecurity education, training and skills development nationally, supported by activities for citizens for that purpose?	1	Do you promote or develop tailored cybersecurity training and activities for different audiences, and do you have timelines and, PPPs, with a defined specific set of resources to support this?	1	Do you engage relevant stakeholders (e.g. the private sector, civil society, academia) in developing cybersecurity training and education activities, that are periodically assessed and updated based on performance indicators and evolving needs?	1	Are there mechanisms (including through your NCSS) that ensure that cybersecurity education and training activities are regularly updated to stay relevant amid emerging technologies, evolving threats, and new legal regulations and national security directives?	1
	5	Have you conducted a study or gap analysis to identify upskilling and reskilling needs to strengthen cybersecurity skills across all relevant audiences?	1	Do you promote dedicated training activities for reskilling or upskilling of the cybersecurity workforce?	1	Have you developed or funded any national activities to reskill interested individuals, such as career changers and unemployed individuals, in cybersecurity?	1	Do you use EU support mechanisms or funding (e.g. the digital Europe programme, the European Social Fund Plus, Horizon Europe) to upskill or reskill the workforce generally or in sector-specific cybersecurity roles (e.g. in healthcare, energy or SMEs)?	1	Do you have mechanisms to quickly adapt upskilling and reskilling programmes in response to evolving cybersecurity workforce needs and labour market trends?	1
	6	Do you actively promote the importance of obtaining cybersecurity certifications in technical, operational and strategic areas and support public administration entities in encouraging their personnel to pursue these certifications?	1	Does your country provide structured pathways for advanced cybersecurity education (e.g. specialised Master's and PhD programmes, recognised certifications and microcredentials)?	1	Has your country established a broader cybersecurity capacity-building ecosystem, including research labs, specialised educational institutions, regular security events (e.g. hackathons) and partnerships with academic and professional bodies to align training with recognised career	1	Do you provide financial and career incentives across the public and private sectors (e.g. scholarships, apprenticeships, internships, guaranteed jobs) to encourage the uptake of cybersecurity degrees, accreditation or certification?	1	Does your country ensure the long-term relevance of cybersecurity education and certifications by supporting activities such as academic centres of excellence and maintaining the alignment of learning programmes with technological advancements, evolving threats and regulatory changes?	1

					frameworks such as the ECSF?					
	7	Do public administration entities recognise the risks of the cybersecurity workforce skills gap at the national and EU levels?	1	Have you identified concrete measures to address the cybersecurity skills gap?	1	Have you implemented concrete measures to address and reduce the cybersecurity skills gap?	1	Do you systematically assess the effectiveness of the measures implemented to close the cybersecurity skills gap?	1	Do you continuously monitor, benchmark and evaluate international best practices to address the cybersecurity workforce skills gap and systematically adapt and integrate those proven measures into the national context through structured stakeholder engagement and policy feedback loops?	1
	8	Have you conducted any formal or informal study – including ad hoc efforts – to identify measures for closing the cybersecurity skills gap?	1	Have priority actions been set out to address the cybersecurity skills gap across different sectors and stakeholder groups?	1	Have stakeholders from the public and private sectors been involved in the identification and prioritisation of policy/activities to address the cybersecurity skills gap?	1	Do you assess the impact of cybersecurity skills development policy/activities across the public and private sectors using performance indicators?	1	Have you conducted or planned foresight exercises to anticipate future challenges and opportunities in cybersecurity workforce development?	1
	9	Has an initial assessment been conducted to establish cybersecurity roles and competencies in line with national workforce planning and frameworks, such as the ECSF and the National Initiative for Cybersecurity Education workforce framework for cybersecurity?	1	Have you established cybersecurity role profiles / job families in your national occupational classification?	1	Have you implemented cybersecurity role profiles / job families within your national workforce development plan?	1	Do you have funding instruments targeting different cybersecurity role profiles or job families based on the current state of the skills gap?	1	Do you continuously update cybersecurity role profiles to reflect technological advancements and align with international and EU frameworks (e.g. the National Initiative for Cybersecurity Education workforce framework for cybersecurity, the ECSF)?	1
	10	Have you formally acknowledged the importance of attracting under-represented	1	Have you conducted a study or assessment of under-represented	1	Have you supported or developed any policies/activities or programmes to	1	Have you implemented or funded any scholarships, outreach or inclusive hiring	1	Do you continuously monitor socioeconomic trends and adapt cybersecurity	1

		groups (e.g. women, minorities, people with disabilities) to pursue a cybersecurity career?		groups in the national cybersecurity market?		encourage under-represented groups to join the cybersecurity field?		campaigns to support under-represented groups in cybersecurity careers?		programmes targeting under-represented groups to ensure their ongoing relevance and effectiveness?	
	11	Has any formal or informal assessment – including ad hoc efforts – been conducted to explore suitable indicators for evaluating the impact of cybersecurity education and training activities?	1	Have you designated a competent authority responsible for coordinating and assessing cybersecurity skills development efforts?	1	Have you set indicators (e.g. on the number of trained professionals, gender balance or employment outcomes) to evaluate the effectiveness of your skills development efforts?	1	Do you regularly evaluate the effectiveness of your skills development efforts based on the set indicators?	1	Do you actively participate in international activities and forums to promote cybersecurity skills development and share best practices?	1
	12	Have you engaged in preliminary discussions with other Member States and EU agencies on how to address the cybersecurity skills gap across the EU?	1	Do you promote EU-level activities aimed at closing the cybersecurity skills gap (e.g. the Cyber Skills Academy, national chapters of Women4Cyber, the digital skills and jobs platform) within your country?	1	Have you adopted measures to support the development of a single market for cybersecurity skills, including activities that enhance workforce mobility and recognition of qualifications across Member States?	1	Do you systematically monitor and evaluate joint cybersecurity skills activities developed in cooperation with other Member States through EU frameworks (e.g. the ECCC) to ensure effectiveness and continuous improvement?	1	Do you lead or actively participate in the EU-wide discussions and forums, sharing national best practices and contributing to joint efforts to close the cybersecurity skills gap?	1

4. Foster Research and Development (R&D) and Innovation

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
4 – Foster Research and Development (R&D) and Innovation	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?		Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Do you recognise the need to support R & D activities dedicated to cybersecurity?	1	Do you have a process to establish national R & D priorities (e.g. emerging topics relating to deterring, protecting against, detecting and adapting to evolving cyber threats)?	1	Do you have mechanisms to incorporate cybersecurity R & D findings into policy and explore opportunities in EU-wide initiatives and funding (e.g. Horizon Europe, the digital Europe programme)?	1	Are there mechanisms to regularly assess that national instruments (e.g. NCCs) have the resources required?	1	Are there mechanisms to ensure the alignment over time of the national cybersecurity R & D priorities with EU strategic policies, objectives and initiatives (e.g. the digital single market, Horizon Europe, the EU cybersecurity strategy, the digital Europe programme, European Digital Innovation Hub calls) and the evolving regulatory frameworks?	1
	2	Do you organise conferences/ workshops to identify effective ways to promote partnerships with academic and research institutions,	1	Are stakeholders from the private sector, the public sector and academic and research institutions involved in establishing national	1	Do you actively promote partnerships that enhance cybersecurity R & D among the private sector, the public sector and academic institutions?	1	Do you have any cooperation agreements in place or incentives with academic and research institutions, potentially involving the private and public	1	Have you established cybersecurity centres of excellence or competence, equipped with advanced predictive analytics and strategic foresight tools,	1

		industry, civil-society organisations and the public sector in fostering cybersecurity innovation?		cybersecurity R & D priorities?			sectors, to support the development and deployment of cybersecurity tools and secure network infrastructure?		to serve as practical, state-of-the-art research and innovation hubs?	
	3	Have you conducted any initial assessments or studies on (semi)automated tools or the integration of innovative technologies (e.g. AI or post-quantum cryptography) into cybersecurity practices?	1	Have strategic objectives, priority areas and key stakeholders been identified to drive national R & D efforts to integrate (semi-)automated tools or any other innovative technologies in cybersecurity solutions?	1	Is there a comprehensive national programme that supports (semi-)automated tools, R & D or the adoption of any other innovative technologies (e.g. AI or post-quantum cryptography), offering incentives and collaboration opportunities to a wide range of public stakeholders and private entities?	1	Do you regularly assess the contribution of (semi-)automated tools or any other implemented innovative technologies to the effectiveness of cybersecurity solutions?	1	Do you actively participate in or lead international- and EU-level forums and discussions on cutting-edge cybersecurity research, innovation and good practices in the use of (semi-)automated tools or any other innovative cybersecurity technologies?	1
	4	Have you conducted a study on implementing responsible data-sharing mechanisms for training users of innovative cybersecurity technologies, while also considering how principles such as open source, standards and interoperability can strengthen these mechanisms?	1	Have guidelines been developed to promote responsible data sharing for training and improving cybersecurity tools with legal and ethical safeguards, incorporating practices that encourage open-source projects, recognised standards and interoperability?	1	Does the national mechanism for responsible data sharing in cybersecurity research and innovation include governance and coordination measures that align with strategic priorities such as open-source collaboration, standards adoption and interoperability?	1	Are national data-sharing mechanisms regularly reviewed and updated to ensure alignment with evolving legal frameworks, ethical standards and operational needs?	1	Do you proactively contribute to international research to develop responsible data sharing for cybersecurity innovations (e.g. open-source initiatives, standards and interoperability), while continuously integrating lessons learned into national innovation policies?	1
	5	Has the integration of the General Data Protection Regulation (GDPR) principles into cybersecurity	1	Has coordination begun between cybersecurity and data protection authorities to align cybersecurity innovation	1	Are there mechanisms in place to ensure that the design, development and use of innovative technology, including AI,	1	Do national cybersecurity innovation programmes include performance indicators or review mechanisms to	1	Do you actively contribute to the development of good practice focused on preserving privacy and	1

		technology development been formally acknowledged in your NCSS or in relevant cybersecurity policy documents?		efforts with privacy requirements?		comply with EU privacy and data protection law (e.g. principles of data accuracy, minimisation, fairness, transparency and data security)?		systematically ensure that GDPR principles are embedded by design and by default in innovative cybersecurity technologies?		data protection in innovative cybersecurity technologies?	
	6	Has the need to embed data protection by design and by default in cybersecurity R & D activities been officially prioritised in a strategic or policy document?	1	Do you provide national guidance for implementing data protection by design and by default in cybersecurity R & D activities?	1	Do you have a mechanism to control the integration of data protection by design and by default into the design of new cybersecurity solutions?	1	Is stakeholder feedback periodically collected to assess and improve national efforts in supporting data protection by design and by default in cybersecurity R & D activities?	1	Do you actively promote and share good practices for data protection by design and by default in cybersecurity R & D activities at the international level?	1
	7	Are there any informal or formal communication channels between national stakeholders (e.g. government agencies, academic and research institutions) and EU and international innovation networks (e.g. ENISA, the ECCC) to share information about cybersecurity R & D opportunities and funding (e.g. calls for consortia, calls for proposals, grants)?	1	Do you have a national framework to guide and coordinate stakeholder participation in EU and international cybersecurity R & D initiatives (e.g. guidelines, contact points, matchmaking platforms)?	1	Do you actively promote or facilitate opportunities for national stakeholders (e.g. government agencies, academic and research institutions) to engage in EU-level or international cybersecurity R & D projects and initiatives?	1	Are there formal agreements or partnerships between your government and other Member States on cybersecurity R & D?	1	Are national stakeholders (e.g. government agencies, academic and research institutions) actively participating in leading international discussions in the area of cybersecurity R & D activities?	1

5. Enhance Incident Preparedness and Response

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
5 – Enhance incident preparedness and response	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have discussions been held to establish a national cyber IPR framework?	1	Has a draft national cyber IPR framework been developed and shared with relevant stakeholders?	1	Is your national cyber IPR framework, as well as associated protocols and cooperation mechanisms, implemented and operational?	1	Do you monitor and regularly update the national cyber IPR framework, associated protocols and cooperation mechanisms to ensure their effectiveness?	1	Is research conducted on improving the cyber IPR framework and its associated protocols or cooperation mechanisms, taking into account future threats and technological changes?	1
	2	Have you initiated the development of national cyber incident response procedures (e.g. standard operating procedures) for identifying, classifying and responding to cybersecurity incidents (including large-scale cybersecurity incidents)?	1	Are national cyber incident response procedures documented and communicated to relevant stakeholders, to effectively identify, classify and respond to cybersecurity incidents?	1	Are national cyber incident response procedures implemented and adopted by relevant stakeholders to ensure efficient cyber incident identification, classification and coordinated response to cybersecurity incidents?	1	Are national cyber incident response procedures regularly reviewed and refined, incorporating input from relevant stakeholders (e.g. feedback and lessons learned, national CSIRTs, EU-level networks such as the European Cyber Crisis Liaison Organisation Network (EU-Cyclone) or the CSIRTs Network)?	1	Do national cyber incident response procedures incorporate threat intelligence and analysis techniques, informed by key national stakeholders and collaborative experience across the EU and other international networks?	1

	3	Have preliminary roles and responsibilities for relevant competent authorities (including law enforcement and sectoral authorities) been outlined in cyber incident response management chain?	1	Have formal roles and responsibilities within the incident response chain been clearly established and communicated to relevant competent authorities, supported by a centralised registry of points of contact across all actors?	1	Are well-defined roles and responsibilities formally established and documented for competent authorities, CSIRTs, law enforcement and sectoral actors to ensure accountability and coordination during cyber incident response, supported by a regularly updated centralised registry of points of contact?	1	Are formal roles and responsibilities within the incident response chain regularly reviewed and optimised to align with national- and EU-level frameworks (including coordination with EU-Cyclone or the CSIRTs Network)?	1	Do the formal roles and responsibilities within the incident response chain allow for dynamic adjustments and flexible public–private collaboration to strengthen response capabilities in evolving threat landscapes?	1
	4	Is the role of CSIRTs as national coordination hubs clearly understood by all relevant stakeholders, ensuring that they recognise the need to provide adequate resources for their operations?	1	Have preliminary efforts been undertaken to estimate and allocate necessary resources to CSIRTs, ensuring that they possess the technical capabilities and staffing required to fulfil their tasks under NIS2?	1	Are CSIRTs fully equipped with adequate resources and staffing to function effectively as national coordination hubs, including meeting the NIS2 requirements for redundancy, secure infrastructure and emergency protocols?	1	Does your CSIRTs' supervisory body regularly monitor, evaluate and adjust CSIRTs' resources and staffing to ensure that they can effectively fulfil their mandate as the national coordination hub?	1	Are CSIRTs employing adaptive strategies and innovative technologies to enhance operational resilience and fulfil proactive tasks (e.g. proactive scanning, risk analysis of future threats)?	1
	5	Has the establishment of joint incident response protocols or trusted communication channels between competent authorities and operators of essential and important entities been initiated?	1	Are preliminary joint incident response protocols under development to facilitate trusted communication and coordinated response between competent authorities and operators of essential and important entities during cybersecurity incidents (in accordance with Article 10 of NIS2)?	1	Are joint incident response protocols documented and operational, ensuring seamless and secure coordination between competent authorities and operators of essential and important entities during cybersecurity incidents, in line with NIS2 cooperation principles?	1	Are joint incident response protocols regularly reviewed and optimised, incorporating lessons learned by both the competent authorities and the operators of essential and important entities?	1	Are joint incident response protocols subject to continuous improvement, including through the use of adaptive methodologies, integration of advanced threat intelligence or new information-sharing tools?	1
	6	Have discussions been held to promote a proactive approach to	1	Are proactive approaches (e.g. the European Cybersecurity	1	Are proactive cybersecurity measures, including advanced	1	Are the proactive cybersecurity measures regularly evaluated and	1	Are the proactive cybersecurity measures continuously adapted,	1

		identifying cybersecurity threats at the national level, focusing on anticipating and preventing incidents (e.g. workshops, studies, exercises)?		Alert System, regular national sectoral exercises, training sessions, awareness-raising campaigns) leveraged to establish frameworks and policies for threat management and coordinated response at the national and EU levels?		detection capabilities, actively implemented, supported by documented processes and stakeholder engagement, to enhance incident handling, reporting, and analysis?		refined, incorporating lessons learned from incidents, exercises and best practices?		utilising innovative tools (e.g. advanced threat intelligence, AI, data analytics) to enhance effectiveness and responsiveness to emerging cyber threats, in line with NIS2 and the Cyber Solidarity Act?	
	7	Is the significance of integrating disaster recovery and continuity of operations recognised within your national cybersecurity preparedness strategy, as encouraged by NIS2 and the Cybersecurity Emergency Mechanism?	1	Has the implementation of policies or pilot programmes been initiated to incorporate disaster recovery and resilience into the NCSS?	1	Are there frameworks in place that include disaster recovery and resilience, with documented procedures and cooperation between competent authorities, essential and important entities and other relevant stakeholders?	1	Is the integration of disaster recovery and resilience strategies regularly monitored, evaluated and improved to ensure comprehensive cybersecurity preparedness, in accordance with NIS2 and EU-level coordination mechanisms?	1	Do disaster recovery and resilience strategies adaptively incorporate cutting-edge practices and innovative technologies to ensure operational continuity against emerging cyber threats, in line with EU-level coordination mechanisms?	1
	8	Is the importance of producing lessons-learned reports after significant cybersecurity incidents acknowledged in initial guidance or strategic planning documents?	1	Have clear procedures been established and applied for conducting lessons-learned reports and root cause analyses, incorporating stakeholder input and aligning with NIS2 requirements?	1	Are structured protocols consistently implemented to document lessons learned across all relevant stakeholders, with outcomes systematically used to strengthen national- and EU-level cybersecurity capabilities?	1	Are lessons-learned outcomes regularly integrated into the NCSS, supported by periodic reviews to ensure continuous improvement and alignment with EU-level coordination?	1	Do lessons-learned processes evolve dynamically, leveraging data-driven insights and advanced analytics to continuously refine and enhance national cybersecurity capabilities?	1
	9	Are plans in place to establish national mechanisms and platforms that are secure and accessible for issuing cybersecurity alerts	1	Have foundational systems or frameworks been developed to enable real-time distribution of cybersecurity alerts and	1	Are national mechanisms fully operational for real-time alerting and threat intelligence sharing, supported by clearly	1	Is the alerting and threat-intelligence-sharing system regularly assessed and integrated with cross-sectoral and EU-level networks (e.g. cross-border cyber hubs,	1	Do alerting mechanisms continuously evolve, leveraging advanced analytics and real-time data capabilities (e.g. AI, data analytics) to enhance threat	1

		and sharing threat intelligence?		threat intelligence sharing?		defined roles and cross-sectoral processes?		EU-Cyclone, CSIRTs) to optimise incident response?		intelligence distribution, in line with NIS2 and the European Cybersecurity Alert System?	
	10	Are there discussions or initiatives aimed at enhancing the role of national CSIRTs as central coordinating bodies, enabling their engagement with EU and global incident response coordination platforms to strengthen situational awareness and international cooperation?	1	Have preliminary frameworks been developed to formalise the roles of national CSIRTs, including their participation in platforms such as ENISA, the CSIRTs Network and other EU-level coordination bodies?	1	Are national CSIRTs operational with adequate resources to manage national cybersecurity incidents and enhance incident response capabilities through collaborative frameworks and participation in EU and global coordination platforms?	1	Is the role of national CSIRTs and their engagement with EU and global coordination platforms regularly reviewed, optimised based on lessons learned from incidents and exercises, and enhanced to strengthen international cooperation?	1	Do national CSIRTs employ innovative threat intelligence and coordination methodologies to adapt in real time to evolving cyber threats and continuously enhance their participation in EU and global platforms by integrating foresight strategies and innovative practices to anticipate and manage international cybersecurity risks?	1
	11	Are there active engagements and discussions aimed at fostering public–private cooperation in cybersecurity, including preliminary meetings to develop sector-specific objectives and measures for IPR?	1	Have cooperative measures been established to improve readiness and incident response, in line with the Cyber Solidarity Act guidelines for joint testing, threat intelligence sharing and clear governance roles between authorities and private entities?	1	Are structured mechanisms, including national cyber hubs, operational and facilitating joint preparedness, real-time response and recovery activities between competent authorities and private entities, leveraging cooperative exercises and secure communication channels?	1	Is public–private cooperation for cybersecurity preparedness, responsiveness and recovery regularly reviewed and optimised, integrating cross-sector resilience measures endorsed by the EU and aligning with coordination policies in the NCSS, through ongoing evaluation processes to refine incident response frameworks?	1	Is public–private collaboration evolving to integrate advanced analytics and innovative tools for anticipating cyber threats, with preparedness and response measures regularly updated based on national evaluations and best practices?	1

3.1.1 Cluster #2: Cooperation and collaboration

6. Address cyber crime

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
6 – Address cybercrime	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Do you have any informal or formal procedures in place to facilitate coordination between law enforcement authorities, judiciary authorities, cybersecurity competent authorities and private sector stakeholders in addressing cybercrime-related activities?	1	Do you have a national framework for detecting, reporting and prosecuting cybercrime that sets out a structured coordination approach involving law enforcement, cybersecurity competent authorities and private sector stakeholders?	1	Is your national legal framework compliant with the EU legal framework on cybercrime (e.g. as regards illegal access to information systems, system interference, data interference, interception and the use of tools to commit offences)?	1	Do you regularly assess whether sufficient human, financial and technical resources are allocated at the national level to combating cybercrime?	1	Is there a mechanism in place to promptly update your national cybercrime strategy or framework in response to emerging cyber threats and trends at the national, regional and global levels?	1
	2	Do you have established cooperation channels (formal or informal) for addressing cybercrime-related topics between	1	Are you developing taxonomies, templates or national initiatives to align the classification of cybercrime incidents between CSIRTs, cybersecurity competent	1	Have you established formal cooperation mechanisms to enable secure and timely information exchange between CSIRTs, cybersecurity competent	1	Are mechanisms in place to assess collaboration between CSIRTs, cybersecurity competent authorities and national law enforcement bodies and to implement	1	Do you actively lead or influence international and EU-level forums and discussions on good practices of cooperation, including cross-border cooperation?	1

		CSIRTs, cybersecurity competent authorities and national law enforcement bodies?		authorities and national law enforcement bodies?		authorities and national law enforcement bodies involved in combating cybercrime?		measures for its enhancement?		
	3	Do you have any informal or formal collaboration mechanisms in place between private sector stakeholders and national authorities to share information on cybercrime-related incidents?	1	Are there national initiatives to strengthen collaboration between public and private sector stakeholders in combating cybercrime (e.g. cooperation networks, joint task forces, trusted information-sharing platforms)?	1	Have you established or designated a central coordinating entity to oversee national efforts in combating cybercrime?	1	Have you established an interinstitutional framework and cooperation mechanisms between all relevant stakeholders (e.g. law enforcement agencies, national CSIRTs and the judiciary), including the private sector (e.g. operators of essential services, service providers) where appropriate?	1	Do you continuously monitor and collect inputs (e.g. emerging cybercrime trends, best practices for cooperation) to dynamically adjust cooperation mechanisms with public and private sector stakeholders?	1
	4	Do you have any informal or formal collaboration mechanisms in place between private sector stakeholders and national authorities to share information on cybercrime-related incidents?	1	Are there policies/activities in your NCCS and/or national initiatives (e.g. cooperation networks, joint task forces, trusted information-sharing platforms) that govern and strengthen collaboration between public and private sector stakeholders in combating cybercrime?	1	Have you established a governance framework that sets out the roles and responsibilities of key stakeholders (CSIRTs, law enforcement agencies and the judiciary) and/or designates a central coordinating entity to oversee national efforts and ensure a coordinated response to cybercrime incidents?	1	Have you established an interinstitutional framework and cooperation mechanisms between all relevant stakeholders (e.g. law enforcement agencies, national CSIRTs and the judiciary), including the private sector (e.g. operators of essential services, service providers) where appropriate?	1	Do you collect disaggregated cybercrime statistics (e.g. operational data, data for trend analysis, financial impact information) and monitor emerging cybercrime trends to regularly inform national policies and adjust cooperation mechanisms with public and private sector stakeholders?	1
	5	Have competent authorities recognised the need to raise awareness among essential and important entities, regarding the identification of cybercrime activities?	1	Have you organised awareness-raising campaigns for essential and important entities aimed at improving the identification of cybercrime activities?	1	Do you provide guidance to essential and important entities on identifying and reporting suspected cybercrime activities?	1	Do you collect statistics on the reporting of cybercrime activities by essential and important entities and use this information to adapt your awareness-raising activities?	1	Do you regularly evaluate and adapt awareness-raising activities for essential and important entities based on emerging cybercrime trends, lessons learned and	1

										feedback from previous campaigns?	
	6	Are there any informal or formal cooperation channels for sharing information on cybercrime activities with cybersecurity competent authorities and law enforcement agencies in other Member States?	1	Have you designated an operational national point of contact to exchange information and respond to urgent information requests from other Member States regarding offences set out in Directive 2013/40/EU on attacks against information systems and Directive (EU) 2016/680 (the Law Enforcement Directive (LED))?	1	Is there a formal mechanism in place to foster cooperation with other Member States and share information to effectively prevent, detect and respond to cybercrime incidents?	1	Do you regularly assess and optimise your participation in European Union Agency for Law Enforcement Cooperation (Europol) cooperation networks (e.g. EC3, the Joint Cybercrime Action Taskforce or the Europol platform for experts)?	1	Do you participate in coordinated actions with other Member States and Europol to disrupt cybercrime activities (e.g. dismantling of organised groups, takedown of criminal infrastructure, dark web markets or botnets) and is there a structured process in place to review the aftermath of these incidents, analysing what went wrong and what went right, to learn lessons and improve future responses to cybercrime?	1
	7	Have you identified the privacy rules you need to comply with during cybercrime investigations?	1	Do you prioritise compliance with personal data protection rules during coordination and information sharing in cybercrime investigations?	1	Are appropriate tools and procedures in place to ensure that information sharing in cybercrime investigations complies with personal data protection rules?	1	During cybercrime investigations, do you consult or leverage guidance from Europol's Data Protection Experts Network to ensure compliance with personal data protection rules?	1	Do you participate in developing and maintaining standardised tools, methodologies, forms and procedures for information sharing during cyber investigations that are shared with EU stakeholders (law enforcement agencies, CSIRTs, ENISA and Europol's EC3)?	1

	8	Have you assessed how key stakeholders combating cybercrime can benefit from the expertise and resources offered by EC3 and ENISA?	1	Has your national 24/7 point of contact for the EU law enforcement emergency response protocol established an information-sharing procedure to get expertise from EC3 during a cyberattack response?	1	Do you cooperate and share information with EU agencies (e.g. Europol's EC3, the European Union Agency for Criminal Justice Cooperation (Eurojust), ENISA) to ensure the effective prevention and detection of, and response to, cybercrime?	1	Do you promote and implement standards and guidelines issued by EC3 or ENISA for collaboration and information sharing (e.g. ENISA's taxonomy for the CSIRT community)?	1	Do you use the EU Blueprint and/or the EU law enforcement emergency response protocol to respond effectively to large-scale cyber incidents?	1
	9	Have you identified the requirements (e.g. knowledge, skills, resources) for law enforcement officials (e.g. police officers, prosecutors, judges) to effectively carry out their duties in the context of cybercrime?	1	Are training materials and programmes on cybercrime-related topics provided at both the national and the EU levels (e.g. by Europol, Eurojust, the European Anti-Fraud Office, the EU Agency for Law Enforcement Training, ENISA) to law enforcement officials?	1	Is specialised training regularly provided to law enforcement officials (e.g. police officers, prosecutors, judges) on cybercrime-related topics (e.g. prosecution of cyber-enabled crimes, collection and handling of electronic evidence, computer forensics)?	1	Do you evaluate the adequacy of the training provided to law enforcement agencies, the judiciary and national CSIRT personnel to address cybercrime?	1	Are there interinstitutional training courses or workshops for law enforcement, judges, prosecutors and national/ governmental CSIRTs at the national level and/or the multilateral level?	1
	10	Have initial measures been implemented to strengthen the detection, investigation and prosecution capabilities of law enforcement and judicial authorities (e.g. police officers, prosecutors, judges) to address cybercrime?	1	Do CSIRTs provide law enforcement and judicial authorities with guidance or support in identifying, reporting or analysing suspected cybercrime incidents?	1	Do law enforcement and judicial authorities have sufficient capabilities (e.g. tools, personnel) to effectively detect, investigate and prosecute cybercrime incidents?	1	Do you have a mechanism in place to regularly evaluate the adequacy of law enforcement and judicial authorities' resources and adjust them as necessary?	1	Do your law enforcement and judicial authorities actively participate in the transborder exchange of best practices and legal expertise (e.g. through the European Judicial Cybercrime Network)?	1

7. Engage in International Cooperation

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
7 – Engage in international cooperation	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Has your government established a formal strategy and/or does it maintain formal or informal cooperation channels with authorities or stakeholders in non-EU countries, expressing the intention to engage in international cooperation on cybersecurity-related issues?	1	Are you engaged in bilateral or multilateral cooperation agreements with Member States, non-EU countries or international partners for purposes such as information sharing, capacity building or the provision of mutual assistance in the field of cybersecurity?	1	Do key national stakeholders (e.g. the ministry of foreign affairs, the national cybersecurity authority, CSIRTs) have sufficient/dedicated means and budget to engage in international cybersecurity partnerships and cooperation frameworks to support strategic alignment on cybersecurity topics?	1	Are international cybersecurity cooperation initiatives regularly assessed for effectiveness and alignment with national- and EU-level objectives (e.g. as per the EU cybersecurity strategy)?	1	Do you take a leading role or engage actively in discussions on one or more topics within multilateral cybersecurity agreements?	1
	2	Do you have any formal or informal coordination or information-exchange channels in place with international partners (beyond the EU's borders) to support the response to large-scale	1	Do you have procedures in place to facilitate the coordination with your international partners to tackle large-scale cybersecurity incidents beyond the EU's borders?	1	Do you actively participate in any international cooperation network or partnership to coordinate and facilitate timely and secure information exchange during large-scale cybersecurity	1	Do you regularly identify lessons learned and areas for improvement from your participation in international cooperation networks and partnerships for incident response beyond the EU's borders?	1	Do you proactively participate in international initiatives that contribute to enhancing the prevention of and response to large-scale cybersecurity incidents (e.g. OSCE confidence-	1

		cybersecurity incidents?				incidents beyond the EU's borders?				building measures, the UN Global Mechanism for Cyberspace) and build trust and confidence with international partners (beyond the EU's borders)?	
	3	Do you have any formal or informal cooperation or cybersecurity information-sharing channels established between key competent authorities (e.g. cybersecurity and NIS2 supervision authorities, cyber crisis-management authorities) and multinational private sector entities operating in your Member State?	1	Are initial steps or negotiations under way to establish formalised reciprocal cybersecurity information-sharing arrangements on threats, vulnerabilities and best practices between key competent authorities (e.g. cybersecurity and NIS2 supervision authorities, cyber crisis-management authorities) and multinational private sector entities operating in your Member State?	1	Do you have established cooperation mechanisms between key competent authorities (e.g. cybersecurity and NIS2 supervision authorities, cyber crisis-management authorities) and multinational private sector entities, and are these mechanisms compliant with national and EU law (e.g. on the sharing of sensitive or classified information)?	1	Do you provide any incentives (e.g. participation in national and cross-border cybersecurity exercises, access to government briefings) to multinational private sector entities to encourage their engagement in cybersecurity information sharing?	1	Do you actively build trust, through secure and reciprocal cybersecurity information sharing, with multinational private sector entities operating in your Member State?	1
	4	Do you officially recognise (e.g. in strategic documents or guidelines) the importance of your national CSIRTs participating in international or regional cybersecurity cooperation frameworks?	1	Do your national CSIRTs plan to or have they already taken initial steps to engage in any international or regional cybersecurity cooperation frameworks beyond the EU's CSIRTs Network?	1	Do your national CSIRTs actively participate in international or regional cybersecurity cooperation frameworks beyond the EU's CSIRTs Network (e.g. the GFCE, the Task Force – Computer Incident Response Team, the International Watch and Warning Network, Forum of Incident Response and Security Teams)?	1	Is the involvement of your national CSIRTs in international and regional cybersecurity cooperation frameworks regularly evaluated to ensure alignment with national priorities and to focus efforts on the most impactful cooperation frameworks?	1	Do your national CSIRTs take a leading role in international CSIRT networks (e.g. the Forum of Incident Response and Security Teams) to drive innovation, share predictive threat intelligence and influence cross-border cybersecurity policies in line with NIS2 principles?	1
	5	Have you officially recognised the need to	1	Do you foster the active participation of national	1	Do you contribute to cybersecurity capacity-	1	Do you conduct regular evaluations of the impact		Have you developed and funded any	1

		actively participate in international cybersecurity capacity-building initiatives targeting EU candidate countries or strategic regions (e.g. the Western Balkans or Eastern Partnership)?		experts or organisations in international cybersecurity capacity-building programmes (e.g. through EU CyberNet)?		building initiatives at the international or regional levels (e.g. GFCE, Global Cyber Alliance, EU CyberNet or Cooperative Cyber Defence Centre of Excellence training)?		and effectiveness of international cybersecurity capacity-building initiatives in which you participate, and adjust your level of involvement on the basis of the findings?		international cybersecurity capacity-building projects, particularly targeting EU candidate countries or strategic regions (e.g. Western Balkans or Eastern Partnership)?	
	6	Do you have an initial plan and specific priority areas for engagement with international organisations and EU agencies (e.g. ENISA, Europol's EC3, the EEAS, the International Telecommunication Union (ITU), the Organisation for Economic Co-operation and Development (OECD), Interpol)?	1	Are roles and responsibilities for engagement with international organisations and EU agencies (e.g. ENISA, Europol's EC3, the EEAS, the ITU, the OECD, Interpol) clearly established and have they been communicated to the competent authorities to ensure effective coordination and compliance with NIS2 requirements?	1	Do you actively participate in cybersecurity-related activities and initiatives led by international organisations and EU agencies (e.g. working groups, cybercrime investigations, development of standards and norms)?	1	Do you regularly evaluate your engagement with international organisations and EU agencies (e.g. ENISA, Europol's EC3, the EEAS, the ITU, the OECD, Interpol) and adjust your involvement based on strategic priorities or lessons learned?	1	Do you proactively lead, chair or initiate activities within international organisations or EU agencies, including leading investigations or proposing new initiatives, to drive strategic priorities, innovation and cross-border coordination in line with NIS2 requirements?	1
	7	Do you acknowledge the value of participating in international and European cybersecurity exercises (e.g. Cyber Europe, Blue OLEx, Locked Shields) for exchanging best practices and enhancing cross-border cooperation?	1	Do you regularly participate in international and European cybersecurity exercises, at least in an observer role?	1	Do you engage with regional organisations (e.g. the EU, NATO) in participating in multinational cybersecurity exercises?	1	Are results of international and European cybersecurity exercises (e.g. Blue OLEx, Locked Shields) regularly assessed to identify areas for improvement in cross-border coordination and operational readiness?	1	Do you organise or contribute to the planning and execution of international or European cybersecurity exercises?	1
	8	Have you conducted any assessment of the alignment of national cybersecurity laws and policy frameworks with	1	Have you identified priority areas (e.g. digital evidence exchange, attribution, cybercrime investigation) for	1	Is there a procedure in place to take part in international discussions to ensure the alignment of the national	1	Are your national cybersecurity legislation and policy frameworks regularly reviewed and updated to ensure	1	Do you actively participate in cross-border initiatives, frameworks and working groups aimed at	1

		international standards, norms and best practices?		harmonising national cybersecurity legislation and policy frameworks with international cybersecurity standards and norms to facilitate international cooperation?		cybersecurity legislation and policy frameworks with international cybersecurity standards, norms and best practices?		ongoing alignment with international cybersecurity standards and norms, while supporting cross-border cooperation and compliance with NIS2 governance requirements?		harmonising cybersecurity norms and standards (e.g. the UN open-ended working group on the security of and in the use of information and communications technologies, the ITU)?	
	9	Have you formally acknowledged the importance of developing norms of responsible state behaviour and confidence-building measures in cyberspace, in alignment with EU and international cybersecurity cooperation frameworks?	1	Have priority areas and key national stakeholders been identified to support national diplomatic efforts in the formulation of a responsible state behaviour framework in cyberspace?	1	Is there a formal framework in place to implement tailored and coordinated diplomatic measures, including attribution and restrictive measures (sanctions), in accordance with the EU cyber diplomacy toolbox?	1	Do you actively participate in joint EU diplomatic responses and operational measures as defined in the EU cyber diplomacy toolbox?	1	Do you lead or actively contribute to international negotiations and discussions on the development of rules, norms and principles for responsible state behaviour in cyberspace, their applicability in international law and confidence-building measures within regional and international organisations (e.g. the UN, OSCE)?	1
	10	Do you officially or unofficially recognise internet fragmentation as a challenge to the global, open and interoperable nature of the internet?	1	Do your NCSS, sectoral policies or guidance documents embed principles that safeguard global, open and interoperable internet, including our core democratic values, fundamental freedoms and human rights online?	1	Do you participate in EU-level initiatives promoting human rights, fundamental freedoms and a secure, open and resilient internet, ensuring inclusive and affordable digital access (e.g. the cybersecurity strategy for the Digital Decade, the European Internet Forum, the Connecting Europe Facility (CEF Digital))?	1	Do you actively engage in structured international partnerships, including with emerging and developing countries (e.g. in the Global South) to promote a global, open and secure cyberspace?	1	Do you lead or actively coordinate international initiatives to strengthen and implement the multistakeholder model for internet governance in global forums (e.g. the UN Internet Governance Forum, the World Trade Organization, the Committee on Digital Economy Policy, the GFCE), shaping norms, policies and cooperative frameworks to ensure a	1

										secure, open and interoperable internet?	

8. Establish Trusted Information-Sharing Mechanisms

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
8 – Establish trusted information-sharing mechanisms	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Has your NCSS acknowledged the strategic importance of establishing trusted information-sharing mechanisms through the development of robust partnerships between public and private stakeholders?	1	Have you created a policy or action plan that sets the scope and priorities for cybersecurity information sharing, identifies key stakeholders and establishes PPPs for trusted information-sharing mechanisms?	1	Do you have a formal information-sharing framework that aligns with EU law and national security priorities, ensuring structured coordination and compliance across relevant stakeholders and incorporating national public–private cooperation mechanisms?	1	Have you optimised your information-sharing framework to distribute tasks among public and private stakeholders (including strategic large-scale private stakeholders), ensuring a high-quality, accurate and timely exchange of information in line with NIS2 requirements and national cybersecurity priorities?	1	Is the national information-sharing framework regularly reviewed and adapted to evolving cybersecurity practices, while ensuring efficient distribution of collected information among relevant public and private stakeholders through advanced data processing technologies such as AI or machine learning?	1
	2	Does your NCSS actively promote and raise awareness about the existence and development of ISACs and PPPs as strategic tools for pooling expertise and resources at the	1	Does your national action plan include the establishment and support of sector-specific cybersecurity information-sharing arrangements such as ISACs and PPPs through dedicated resources provided to facilitate their	1	Are essential and important entities actively encouraged and supported by national authorities to participate in sectoral ISACs through regulatory, technical and financial support to ISACs and PPPs to enable their	1	Do you regularly evaluate the performance and impact of established ISACs to review and adapt the support provided to them to optimise their cooperation and capacity for pooling expertise and resources?	1	Do you regularly integrate outcomes from sectoral ISACs into national strategies and operations while collaborating with ISACs and PPPs to ensure that their activities adapt to evolving threats through joint planning, cross-	1

		national and EU levels?		activities and enable pooling and sharing of information and resources?		strategic role as defined in your NCSS?				sector coordination and alignment with EU initiatives?	
	3	Have you conducted an assessment to identify the need for differentiated access levels among key stakeholder groups such as competent authorities, critical infrastructure operators, law enforcement and private sector actors?	1	Are the roles, responsibilities and access control measures clear and documented for all relevant stakeholders, competent authorities, critical infrastructure operators, law enforcement and private sector actors?	1	Are there guidelines in place setting out the type and level of information that an entity should be able to access based on its maturity level, ensuring that it receives useful, relevant and actionable information?	1	Do you regularly review and update the responsibilities and access control procedures of stakeholders participating in information sharing?	1	Do you maintain formal, cross-sectoral agreements or protocols that specify and periodically adjust institutional access to shared cyber-threat and -incident data, based on evolving operational roles, legal mandates and strategic priorities?	1
	4	Do you recognise the need to protect entities that voluntarily share sensitive cybersecurity information, including basic confidentiality expectations?	1	Are draft legal provisions or policy measures in place that cover liability, confidentiality and GDPR compliance for voluntary information sharing?	1	Are legal safeguards formally adopted and documented, including liability protections and confidentiality protocols for entities sharing sensitive information voluntarily?	1	Are legal safeguards regularly reviewed and updated in coordination with data protection authorities and cybersecurity stakeholders to ensure alignment with evolving national and EU law?	1	Do you maintain cross-sectoral agreements or national-level guidance that clarify legal protections and confidentiality standards for voluntary information sharing, and are these integrated with EU-level mechanisms (e.g. EU-level ISACs, the CSIRTs Network, EU-Cyclone)?	1
	5	Do you maintain any formal or informal cooperation channels between competent authorities and private sector entities responsible for critical infrastructure (i.e. essential and important entities under NIS2 and critical entities under the CER Directive)?	1	Do you have a national cooperation framework focused on the security of critical infrastructure, such as advisory boards, steering groups, forums or expert groups?	1	Do competent authorities and private sector entities involved in critical infrastructure actively participate in the cooperation framework?	1	Do you assess the effectiveness and limitations of cooperation frameworks in fostering cooperation between competent authorities and private sector entities and use the findings to optimise processes?	1	Do you regularly update strategic cooperation agreements or protocols with critical infrastructure operators that enable joint threat analysis, coordinated response planning and integration with EU-level mechanisms (e.g. EU-level ISACs, EU-Cyclone, the CSIRTs Network)?	1

	6	Does the NCSS establish roles and responsibilities for sharing essential national cybersecurity information with relevant private entities?	1	Have clear guidelines and conditions been documented for how different types of national cybersecurity information will be shared with relevant entities?	1	Is information on cyber threats, vulnerabilities and national security status regularly exchanged with private sector entities, particularly those operating critical infrastructure?	1	When sharing sensitive national security information (e.g. intelligence or cybercrime findings), are recipients selected based on confidentiality and the need-to-know principle?	1	Do formal and regularly reviewed protocols or agreements exist that ensure secure, timely and context-specific sharing of national security-related cyber information with critical infrastructure entities?	1
	7	Have you identified benefits that could motivate private entities to actively participate in wider information-sharing initiatives?	1	Have you established a framework for private sector entities that provides incentives – such as early warnings, official threat briefings and participation in joint exercises – for their active involvement in information-sharing mechanisms?	1	Do you actively promote incentives for private sector entities to encourage their engagement in information sharing?	1	Do you provide a sufficiently diverse set of incentives (e.g. technical, financial and intelligence-based) to engage a wider range of private sector entities in information-sharing mechanisms?	1	Do you regularly refine the available incentives to ensure that they remain attractive and effective for target private sector entities?	1
	8	Does your NCSS contain strategic goals aimed at supporting SMEs and small organisations in accessing nationwide or sectoral information-sharing mechanisms in order to enhance collective resilience?	1	Do you have mechanisms in place to reach out to SMEs and small organisations to provide cybersecurity-relevant information, at least on an ad hoc basis?	1	Does your information-sharing framework include mechanisms providing SMEs with access to certain levels of information?	1	Do you have mechanisms in place to ensure that SMEs and small organisations can effectively benefit from information sharing with major organisations?	1	Does your information-sharing framework enable the dynamic distribution of relevant information across sectors and entity types, ensuring that insights from more mature entities are effectively shared with others?	1
	9	Have you assessed the availability of secure voluntary information-sharing platforms with clear cross-sector responsibilities for stakeholders to be incorporated into your NCSS?	1	Does your NCSS encourage integration of inputs collected and centralised by a national stakeholder from law enforcement, intelligence, CSIRTs and the private sector to build a unified threat landscape view?	1	Have you established and operationalised, through formal guidance from CSIRTs, cooperation platforms that enable real-time and secure information exchange among stakeholders?	1	Do you regularly evaluate and refine the effectiveness of your information-sharing sources, procedures, tools and platforms to ensure that they support secure and coordinated exchange through dedicated channels among law enforcement,	1	Do you use advanced information-sharing tools that combine real-time threat intelligence, AI-driven analysis, and secure cross-border exchange, that are regularly updated to stay scalable, responsive to new threats, and able to produce actionable	1

								CSIRTs and private entities?		insights for national and EU-level decision-making?	
	10	Is the need to address legal, organisational and cultural barriers to information sharing formally acknowledged in your NCSS or policy documents?	1	Are there ongoing initiatives to reduce legal, organisational or cultural barriers and thereby foster effective information sharing?	1	Do you support expert exchange programmes, joint exercises or participation in events to actively overcome cultural barriers and foster information sharing?	1	Are legal and organisational frameworks regularly reviewed and adapted in consultation with cross-sector stakeholders to reduce barriers to information sharing?	1	Do you maintain cross-sector and cross-border cooperation mechanisms that proactively address emerging legal and organisational barriers, incorporating lessons learned from joint exercises and EU-level collaboration?	1

9. Establish Mutual Assistance Processes

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
9 – Establish mutual assistance processes	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Is there an initial awareness among national stakeholders about the need for mutual assistance in supervisory and enforcement actions under NIS2?	1	Have you identified key national and cross-border stakeholders (including CSIRTs, law enforcement agencies and sectoral regulators) for cooperation in supervisory and enforcement measures (including specialised support and expertise)?	1	Have you established formal mutual assistance agreements with other Member States covering areas such as incident response, legal proceedings and sharing of cybersecurity capabilities?	1	Do you have a mechanism to assess the effectiveness, efficiency and consistency of supervisory and enforcement measures, implemented under mutual assistance agreements?	1	Are best practices in cross-border supervisory and enforcement cooperation continuously reviewed and integrated into national processes?	1
	2	Has a preliminary legal analysis been conducted to identify national provisions relevant to mutual assistance under NIS2?	1	Are legal experts regularly consulted when planning or conducting mutual assistance activities related to supervisory and enforcement measures?	1	Do you have any legal mechanisms in place to ensure that supervisory and enforcement measures under mutual assistance are in line with national and EU law?	1	Are mutual assistance activities related to supervisory and enforcement regularly evaluated for legal compliance and updated accordingly?	1	Are lessons learned from mutual assistance activities regarding supervision and enforcement systematically used to improve your legal framework and to enhance the timeliness and security of responses?	1
	3	Are formal or informal points of contact	1	Have you designated a single point of contact	1	Are secure and reliable communication channels	1	Are the single points of contact and	1	Are lessons learned from previous mutual	1

		established for mutual assistance with other Member States?		within your competent authorities for the purpose of mutual assistance coordination?		available for mutual assistance among competent authorities?		communication channels regularly tested for reliability and operational efficiency?		assistance requests used to improve communication and coordination capabilities?	
	4	Have you considered developing templates and protocols to facilitate mutual assistance requests and their handling?	1	Are standardised templates available for submission and handling of mutual assistance requests?	1	Are procedures documented for submitting, responding to and documenting mutual assistance requests?	1	Do you regularly review the procedures and adapt them accordingly, especially to ensure proportionality, competence alignment and respect for sovereignty?	1	Are mechanisms in place to ensure that mutual assistance procedures remain relevant in light of technological developments, legal changes and evolving security directives?	1
	5	Do you have any formal or informal cooperation practices among competent authorities to consult, inform and support each other in cross-border supervisory and enforcement actions?	1	Are initial procedures in place to facilitate regular consultation and information exchange among competent authorities for mutual assistance activities?	1	Have documented guidelines been developed to support consistent implementation of mutual assistance processes and ensure clarity among competent authorities?	1	Do you have a mechanism to support cross-sectoral and cross-domain (e.g. civilian and defence) consultation and coordination in cross-border supervisory and enforcement actions?	1	Are existing cooperation networks (e.g. the NIS2 Cooperation Group) and/or participation in specific programmes (e.g. staff exchange) used to consult, inform and support Member States in supervisory and enforcement measures, contributing to a coordinated cybersecurity approach and strengthening mutual understanding?	1
	6					Do you use the NIS2 Cooperation Group as a platform to discuss specific requests for mutual assistance to enhance cooperation at the EU level?	1				
	7	Have you reviewed existing best practices in supervisory and enforcement measures to support national mutual	1	Do your competent authorities have internal procedures or guidelines in place to request mutual assistance from	1	Do you have a process in place to request or provide mutual assistance through the Cybersecurity Emergency Mechanism?	1	Do competent authorities have established processes to handle specific cybersecurity requests, such as on-site inspections, off-site	1	Do you proactively use EU resources (e.g. ENISA's cybersecurity support action) to strengthen cross-border mutual assistance in	1

		assistance processes?		other Member States under NIS2?				supervision or targeted security audits?		supervisory and enforcement activities?	
	8	Has your government informally or formally recognised the need to allocate sufficient resources to support effective mutual assistance in supervisory and enforcement actions under NIS2?	1	Are resources (personnel, budget or tools) currently allocated to mutual assistance activities?	1	Is proportionality taken into account when allocating resources (personnel, budget or tools) for mutual assistance activities?	1	Are regular evaluations conducted to ensure that sufficient and proportionate resources (personnel, budget or tools) are dedicated to mutual assistance activities?	1	Are lessons learned from previous mutual assistance activities used to assess and adjust future resource allocations?	1
	9	Are there any formal or informal channels for sharing information or coordinating inspections/audits with other Member States under the NIS2 mutual assistance framework?	1	Have you initiated joint supervisory or inspection activities with other Member States or participated in early-stage coordinated audits, as part of mutual assistance or cooperation efforts?	1	Are common agreements or arrangements in place to conduct joint supervisory actions, inspections or audits with other Member States?	1	Do you monitor and evaluate the effectiveness of joint supervisory actions, inspections and audits to identify areas for improvement?	1	Are lessons learned and best practices from joint supervisory actions, inspections and audits actively shared in the NIS2 Cooperation Group or in other EU networks to adapt national processes?	1
	10	Have you identified potential situations in which a request for mutual assistance might be refused?	1	Are clear conditions established under which a mutual assistance request may be refused due to a lack of competence or because the request is disproportionate to the supervisory tasks of the competent authority?	1	Are clear conditions established under which a mutual assistance request may be refused if it concerns information or actions contrary to national security, public security or defence interests?	1	If considering the refusal of a request, do you have processes to consult the other concerned competent authorities?	1	If considering the refusal of a request and upon the request of the concerned Member States, are there procedures in place to consult the European Commission and ENISA?	1

3.1.2 Cluster #3: Cybersecurity governance

10. Develop Crisis Management Frameworks

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
10 – Develop crisis management frameworks	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Has the need to establish a national cyber crisis-management framework been anchored in a national strategic or policy document?	1	Have you proposed a national cyber crisis-management framework outlining key processes, stakeholder roles, responsibilities and accountability structures?	1	Is a dedicated cyber crisis-management framework established and integrated within your overall national crisis-management framework, including business continuity and disaster recovery aspects?	1	Is the national cyber crisis-management framework regularly reviewed and updated based on stakeholders' feedback, lessons learned and international best practices?	1	Do you apply foresight techniques and integrated innovative approaches to systematically update your national cyber crisis-management framework, ensuring its effectiveness against emerging and future cyber threats?	1
	2	Is there any formal or informal recognition that cyber crisis response should be coordinated with national crisis-management structures?	1	Have draft plans, coordination guidelines or working groups been established to explore the alignment between cyber crisis-management and national crisis-management mechanisms?	1	Is cyber crisis management formally defined and integrated into the national crisis governance framework with clear information on roles and responsibilities and coordination protocols,	1	Is the integration of cyber crisis management into the national crisis governance framework regularly reviewed to ensure that both systems stay aligned when changes occur?	1	Is the alignment between cyber crisis management and general crisis management continuously refined through joint exercises, feedback loops and scenario-based planning involving	1

						including cross-border aspects?				relevant national- and EU-level actors?	
	3	Were initial steps taken to introduce predefined response plans tailored to different cybersecurity threat scenarios?	1	Are predefined incident response plans for various threat scenarios formally established and regularly updated?	1	Do you have structured processes to train and coordinate relevant authorities and stakeholders for effective implementation of incident response plans?	1	Are incident response plans regularly evaluated and enhanced based on feedback from relevant stakeholders and international best practices?	1	Are incident response plans dynamically updated based on predictive insights and lessons learned, ensuring continuous improvement and fostering innovation in cyber crisis management?	1
	4	Is there a preliminary approach to selecting competent authorities for managing large-scale cybersecurity incidents, outlining roles and responsibilities for public and private stakeholders and ensuring adequate resources for national cyber crisis management?	1	Is there a structured approach that ensures that competent authorities are formally nominated and introduced to all relevant stakeholders and actively engage in cyber crisis management with national actors (e.g. security, defence, civil-protection and law enforcement agencies, ministries), with the necessary resources to fulfil their mandate?	1	Is there a designated authority with a clear legal mandate and with adequate and sustainable human, financial and technical resources, and have clear roles and responsibilities been formally established for all stakeholders to ensure structured and efficient collaboration in managing large-scale cybersecurity incidents and crises?	1	Is there a systematic mechanism that ensures that competent authorities regularly review their legal mandate, resources and capabilities, to maintain the full alignment of stakeholders with their roles and responsibilities, through continuous evaluation and adjustment of resource adequacy and to guarantee effective coordination and response during large-scale cybersecurity incidents and crises?	1	Is there a flexible, dynamic and forward-looking mechanism that ensures that specialised resources are in place for continuous forward planning, threat anticipation and adaptive planning, and that roles and responsibilities are regularly reviewed and optimised based on evolving threats and lessons learned?	1
	5	Is there a common understanding among stakeholders of the importance and value of conducting exercises to test and improve national cyber crisis-management capabilities?	1	Are cybersecurity crisis exercises and simulations covering the strategic, operational and technical levels organised nationally, at least on an ad hoc basis?	1	Are sector-specific exercises, including tabletop and live simulations, regularly held at the national and/or international levels to test crisis management, assess preparedness, identify gaps and validate coordination protocols,	1	Is there a multi-year cybersecurity exercise programme with dedicated funding for design, planning and execution, including procedures to collect, review and implement feedback to meet participants' needs?	1	Are national cybersecurity exercise scenarios and procedures regularly updated and harmonised with other Member States to reflect technological advances, evolving threats, global developments and	1

						with documented outcomes and stakeholder involvement?				integration into European crisis response mechanisms?	
	6	Do you acknowledge the value of participating in EU-level, regional and international exercises and simulations (e.g. Cyber Europe, Blue OLEx, Locked Shields) for sharing best practice and enhancing cooperation across sectors and borders?	1	Do you participate in cyber crisis-management exercises at the EU level at least in an observer role?	1	Do you actively engage in EU-level, regional or international cyber crisis exercises?	1	Do you actively encourage both public and private stakeholders to participate in EU-level cybersecurity simulations to test and optimise coordination protocols across sectors and borders?	1	Do you organise or actively contribute to the organisation of tabletop and live simulations at the EU level to lead and innovate cross-border cyber crisis-management capabilities?	1
	7	Is there an initial recognition of the value of systematically gathering lessons learned from exercises and real-world incidents to improve national cyber crisis-management capabilities?	1	Have procedures or guidance been initiated to document lessons learned from cyber crisis exercises and integrate them into future planning efforts?	1	Are after-action and evaluation reports systematically produced following cyber crisis exercises and incidents to document outcomes and lessons learned?	1	Is there an established lessons learned process to systematically collect, analyse and integrate insights from cyber crisis exercises and incidents into national cyber crisis-management practices?	1	Are lessons learned from cyber crisis exercises and real-world incidents systematically reviewed and integrated into national cyber crisis-management frameworks through formal evaluation cycles and stakeholder consultations?	1
	8	Is the importance of sector-specific cyber crisis planning or public–private coordination acknowledged in national strategic documents?	1	Are frameworks being developed to support sector-specific cyber crisis plans, aimed at promoting preparedness in critical sectors and strengthening public–private coordination at the operational level?	1	Is there active engagement with sector representatives, including critical operators not regulated under NIS2, through regular meetings or forums to collaboratively develop and maintain cyber crisis plans, ensuring ongoing coordination between competent authorities and private entities?	1	Are sector-specific cyber crisis plans systematically updated and integrated into the broader national cyber crisis plan, incorporating feedback from both public and private stakeholders?	1	Are insights from emerging threats and technological advancements systematically leveraged to continuously enhance sector-specific cyber crisis preparedness and PPPs?	1

	9	Is there any formal or informal expectation or general awareness that public entities and critical, essential and important entities should maintain continuity and recovery capabilities in the case of cyber incidents?	1	Are national guides or draft initiatives available to support critical, essential and important entities in developing business recovery plans (BRPs), including references to frameworks such as ISO 22301, NIST special publication 800-34 or the control objectives for information and related technology (COBIT) framework?	1	Is there a structured BRP framework in place, developed in consultation with relevant stakeholders, based on recognised reference models (e.g. ISO 22301, NIST special publication 800-34 or the COBIT framework), with specified procedures for resumption and recovery?	1	Are BRPs regularly reviewed and updated based on lessons learned from incidents and exercises, with national authorities providing tailored guidance to different types of entities?	1	Are BRPs systematically integrated into broader national continuity and resilience planning, ensuring adaptation driven by forward planning and cross-sectoral coordination?	1

11. Secure Digital Identity and Build Trust in Digital Public Services

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
11 – Secure digital identity and build trust in digital public services	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Has a gap analysis been conducted to identify specific requirements for transforming public administrations and digital public services?	1	Have strategic guidelines (e.g. high-level policies, general principles or technical standards) been developed to ensure cybersecurity, efficiency, accessibility and compliance with EU standards for digital public services?	1	Are cybersecurity policies consistently implemented and supported by an established governance framework across public administrations to enhance trust in digital public services?	1	Are cross-sectoral strategic coordination efforts in place to allow continuous feedback, update mechanisms and/or framework formalisation to maintain the required level of cybersecurity effectiveness and trust in digital public services?	1	Have strategic decisions been taken to ensure that digital public services are secure by design, to foster a culture of innovation and cybersecurity in public administrations and to ensure that digital public services are driven by continuous monitoring and predictive analytics (or similar techniques)?	1
	2	Does your NCSS include requirements that outline high-level security and privacy measures to protect sensitive information in national digital identity systems and ensure reliable identification?	1	Do you have a strategy and/or guidelines to develop or promote national digital identity systems and trust services (e.g. e-signatures, e-seals, e-registered delivery services, time stamping, website authentication) for citizens and businesses that are in line with European and international norms on	1	Are secure and reliable digital identity solutions developed with participation from both public stakeholders (e.g. cybersecurity and NIS2 supervision authorities, the European Commission, ENSIA) and private stakeholders, in line with	1	Have you implemented mutual recognition of e-identification means with other Member States?	1	Do you participate in peer reviews as part of e-identification schemes, to maintain high levels of security, privacy and interoperability, adapting to new technological developments and emerging threats?	1

				security, privacy-by-design and interoperability?		guidelines to ensure effective cross-border interoperability and robust security and privacy protections?					
	3	Have you set out data security requirements for digital public services in a relevant strategic or policy document?	1	Are high-level policies, general principles or technical standards in place to ensure the secure management of sensitive data exchanges in digital public services?	1	Are national policies for data security and protection implemented and operational across digital public services?	1	Are strategic coordination efforts in place across sectors to ensure data security in digital public services?	1	Are strategic decisions to enhance trust in digital public services driven by continuous monitoring and forward planning?	1
	4			Have formal discussions or practice-sharing sessions been conducted with key stakeholders on transparent data management in digital public services?	1	Is there a structured approach in place to ensure transparent data exchange practices within digital public services?	1	Are public trust surveys conducted to assess the impact of digital public service activities on citizens' trust?	1	Do you implement an adaptive approach to enhancing data security in digital public services?	1

12. Establish National Level Risk-Assessment

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
12 – Establish national level risk-assessment	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Is there recognition that your NCSS should follow a comprehensive, all-hazards, risk-based approach to identifying and managing cybersecurity risks?	1	Has a draft national methodology for cyber risk assessment been developed or piloted for priority sectors, such as those listed in Annexes I and II to NIS2, or CER Directive critical entities?	1	Is your national cyber risk assessment methodology aligned with internationally recognised standards (e.g. ISO 31000, ISO/IEC 27005) or ENISA guidance?	1	Does your national cyber risk assessment methodology ensure coordinated identification and management of risks to essential and important entities, while also integrating with other Member States' risk assessments and critical entity resilience assessments?	1	Is your national cyber risk assessment framework flexible enough to adapt to the evolving cybersecurity threat landscape?	1
	2	Has your national regulatory framework incorporated requirements for identifying critical, essential and important entities?	1	Have you established processes to ensure that all relevant stakeholders understand their roles and responsibilities in identifying these entities and their associated assets?	1	Do formal mechanisms exist to coordinate asset identification and risk assessments across sectors as part of your national resilience and cybersecurity strategies?	1	Is there a structured process to regularly review and update the list of relevant entities and associated assets to remain aligned with the requirements of NIS2 and the CER Directive?	1	Does your national asset inventory deliver a complete and detailed view of critical entities, covering everything from high-level services to technical components?	1
	3	Do you ensure that stakeholders are aware	1	Have procedures been established to regularly	1	Is there a centralised and regularly updated	1	Is there a mechanism in place to ensure that the	1	Are formal procedures in place for cross-sectoral	1

		that the inventory of critical assets must be continuously updated to maintain comprehensive coverage in the national cyber risk assessment?		compile and update inventories of critical assets, including physical, digital and hybrid systems, to support national cyber risk assessments?		inventory of critical assets managed by the designated competent authority?		inventory of assets supporting critical, essential and important entities is systematically updated?		validation, inter-agency data sharing and integration of the asset inventory into national- and EU-level resilience planning processes?	
	4	Have you established high-level requirements that mandate the use of scientific and technological methods (e.g. quantitative risk modelling, threat simulations, AI-driven analytics) in cyber risk management?	1	Do national initiatives or guidelines promote the use of structured methodologies or tools (e.g. threat modelling, vulnerability scanning) in cyber risk assessments?	1	Is the national cyber risk assessment process based on scientific and technological methodologies and applied consistently across all relevant sectors?	1	Are formal mechanisms in place to ensure that cyber risk assessments are regularly updated using validated scientific models, sector-specific data and coordinated cross-sector approaches?	1	Do you actively participate in the development of scientifically and technologically grounded cyber risk assessment processes and share best practices with other Member States?	1
	5	Do relevant stakeholders acknowledge that national cyber risk assessment findings should guide strategic resource coordination to reduce the likelihood and impact of cyber incidents on critical entities, in line with NIS2 and the CER Directive?	1	Have you initiated programmes or planning efforts to align resource coordination with cyber risk assessment findings?	1	Are the results of cyber risk assessments systematically used to guide national resource planning, threat monitoring and mitigation strategies?	1	Are there formal mechanisms to coordinate resources and authorities across sectors based on cyber risk assessment outputs and performance indicators?	1	Is resource coordination informed by real-time cyber threat intelligence to support flexible and agile responses to evolving threats?	1
	6	Is there any informal or formal procedure among national stakeholders to ensure that the evolving cyber threat landscape informs updates to national cyber risk assessments?	1	Does your national cyber risk assessment framework include formal mechanisms to collect and integrate lessons learned from cyber incidents and exercises?	1	Is there a formal feedback mechanism to ensure that cyber risk assessments are updated based on incident notifications, threat intelligence and lessons learned from exercises?	1	Are lessons learned from cyber incidents and exercises systematically integrated into national cyber risk assessments through a formal review process?	1	Is your national cyber risk assessment continuously updated with new inputs, including emerging threats and lessons learned from cyber incidents and exercises, to ensure an accurate reflection of your	1

									national cyber risk posture?	
	7	Do national authorities engage, even on an ad hoc basis, in activities such as workshops or roundtables to align cybersecurity strategy objectives with national security priorities?	1	Are there ongoing initiatives or documented efforts to systematically align national cybersecurity objectives with national security priorities?	1	Is the NCSS explicitly based on a comprehensive cyber risk assessment that incorporates national security considerations?	1	Are formal mechanisms in place to ensure ongoing alignment between cybersecurity strategy objectives and evolving national security risks?	1	Are national cyber risk assessments regularly updated using scenario planning and simulations that account for geopolitical, technological and hybrid threat developments?	1
	8	Are formal or informal practices used to identify key cybersecurity challenges through national-level cyber risk assessments?	1	Have any formal or informal methods been established to prioritise key cybersecurity challenges based on the outcomes of national cyber risk assessment?	1	Are cybersecurity priorities systematically derived from national cyber risk assessment outcomes and integrated into strategic planning and resource allocation?	1	Are cybersecurity prioritisation decisions based on formal criteria and performance indicators, and coordinated across essential and important entities, critical sectors and competent authorities?	1	Are up-to-date results of national cyber risk assessments systematically made available to decision-makers to support informed cybersecurity-related strategic decisions?	1
	9	Do national stakeholders have a common understanding of the importance of conducting periodic cyber risk assessments that address threats, vulnerabilities and impacts on critical sectors and essential entities?	1	Have initial efforts or pilot projects been launched to assess interdependencies and cascading effects across critical sectors as part of national cyber risk assessment practices?	1	Are national cyber risk assessments conducted regularly and comprehensively, addressing threats, vulnerabilities, interdependencies and cascading effects?	1	Are cyber risk assessments embedded within national planning processes, supported by cross-sector collaboration and formal review cycles?	1	Are national cyber risk assessments continuously updated using advanced methodologies – such as real-time data, simulations and strategic foresight – to anticipate cascading impacts on critical entities, in alignment with NIS2 and the CER Directive?	1
	10	Have competent authorities and priority sector entities begun collaborating to develop sector-specific guidance for cyber risk assessments under NIS2 and the CER Directive?	1	Are all relevant stakeholders, including critical entities, digital service providers and SMEs, actively engaged in national and sectoral cyber risk assessments to create a comprehensive threat landscape?	1	Are sector-specific methodologies and tools consistently applied across priority sectors, with structured participation from critical entities, service providers and SMEs?	1	Are cyber risk assessments formally coordinated across sectors, ensuring data sharing and integration into the national threat landscape analysis?	1	Are sectoral cyber risk assessments continuously updated using real-time threat intelligence, predictive analytics and collaborative mechanisms with national and cross-border stakeholders?	1

	11	Has a plan been drafted to provide tools, training and guidance to support relevant competent authorities and critical, essential and important entities in conducting cyber risk assessments?	1	Have training programmes, standardised templates or sector-specific tools been developed or initiated to enhance the capacity of competent authorities and critical, essential and important entities to conduct consistent cyber risk assessments?	1	Are tools, training and guidance systematically provided to relevant competent authorities and critical, essential and important entities under national oversight and quality assurance mechanisms?	1	Are capacity-building measures integrated into national cybersecurity planning and supported by formal evaluation mechanisms and cross-sectoral coordination?	1	Is capacity-building continuously enhanced through feedback mechanisms, innovation programmes and lessons learned from cyber exercises and cyber incidents?	1
	12	Is there a high-level structure or organogram that makes clear the roles of relevant competent authorities and critical, essential and important entities in conducting cyber risk assessments?	1	Do you have a draft framework that allocates responsibilities to national and cross-border stakeholders for cyber risk assessment, incident handling and operational resilience?	1	Are structured mechanisms in place for coordinated cyber risk assessments and mitigation by relevant competent authorities and critical, essential and important entities, with roles and responsibilities clearly established in national policy or legal frameworks, communicated to all stakeholders and supported by shared methodologies?	1	Are formal cooperation frameworks in place to support joint cyber risk assessments and information sharing among relevant competent authorities and critical, essential and important entities, with responsibilities operationalised through formal agreements, joint protocols or inter-agency coordination mechanisms?	1	Does the national framework include an advanced tool that enables relevant competent authorities and critical, essential and important entities to conduct cyber risk assessments, aggregate results and provide up-to-date data for different management levels, while ensuring that roles and responsibilities are regularly reviewed and updated in line with evolving threats, lessons learned and strategic foresight?	1
	13	Are there any formal or informal practices for using cyber risk assessment results in national cybersecurity planning and resource allocation (Articles 18–20 of NIS2)?	1	Have you aligned cyber risk assessment outcomes with updates to your NCSS and with strategic planning or resource allocation for cybersecurity risk management?	1	Are cyber risk assessment findings systematically integrated into your strategic planning, policy development and capability-building programmes?	1	Are formal mechanisms in place to ensure that cyber risk assessment outcomes directly inform national strategic priorities, resource allocation and the development of cybersecurity capabilities?	1	Are cyber risk assessment results continuously used in processes driven by forward planning to dynamically inform the NCSS and sectoral frameworks, support risk-informed resource allocation and enhance the operational resilience and	1

										cybersecurity capabilities of critical, essential and important entities?	

13. Strengthen National Cybersecurity Governance

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
13 – Strengthening national cybersecurity governance	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Has a national cybersecurity governance structure been formally designated under the Cyber Solidarity Act, NIS2 or another legal cybersecurity framework, with an identified lead authority responsible for coordination across sectors?	1	Is a documented governance model in place that clearly establishes roles, responsibilities, decision-making processes and coordination mechanisms and allocates roles and responsibilities to competent authorities (e.g. national competent authorities, national cybersecurity certification authorities, NCCs), CSIRTs and relevant sectoral stakeholders?	1	Is a formal governance framework in place that clearly sets out roles, responsibilities and interactions between all key stakeholders and organisations?	1	Are governance structures routinely reviewed, with responsibilities aligned across ministries, agencies and sectors through binding mechanisms?	1	Is the governance framework regularly updated to address emerging risks and stakeholders and to integrate foresight capabilities?	1
	2		1	Are coordination mechanisms under development (e.g. draft memorandums of understanding, informal communication channels)?	1	Are there formal coordination frameworks in place enabling structured collaboration among CSIRTs, single points of contact and competent authorities as	1	Is collaboration institutionalised through joint activities, incident exercises or shared platforms with harmonised procedures?	1	Are coordination mechanisms flexible and scalable, adapting to new threats, technologies and cross-border challenges	1

					defined in Article 13 of NIS2?				through continuous improvement?	
	3	Are there basic planning structures or at least ad hoc working groups overseeing NCSS implementation?	1	Is there an action plan with timelines and roles to support structured implementation of the NCSS?	1	Is NCSS implementation managed through a central governance body with oversight, monitoring and reporting functions?	1	Are planning and implementation activities coordinated through cross-sector platforms and aligned with national digital policies?	1	Is the strategy implementation continuously monitored, evaluated and optimised using strategic foresight and data-driven performance indicators?	1
	4	Are cybersecurity and sectoral authorities aware of the need to collaborate on risk and threat management?	1	Are initial efforts in place to build bridges between cybersecurity bodies and sector-specific authorities (e.g. critical infrastructure)?	1	Are coordination structures operational, ensuring that cybersecurity is embedded in sectoral regulatory frameworks (e.g. covering transport or energy), as per Article 13(4) of NIS2?	1	Are dialogue mechanisms formalised and aligned with sectoral crisis management or operational continuity protocols?	1	Is coordination driven by integrated national risk assessments and reviewed in light of joint simulations or multisector threat intelligence?	1
	5	Have you identified the need to periodically assess capabilities of national cybersecurity authorities across human, technical and financial dimensions?	1	Have any ad hoc, pilot or preliminary capability assessments been conducted across relevant national cybersecurity authorities (e.g. the national cybersecurity certification authority for the peer-review exercise)?	1	Are regular, structured capability assessments conducted across national cybersecurity authorities, including the identification and prioritisation of capability gaps?	1	Are the results of capability assessments used to shape national training, staffing and resourcing policies across national cybersecurity authorities?	1	Are assessments forward-looking, benchmarking against best practices and feeding into long-term resilience and workforce development planning?	1
	6	Are supervisory activities (e.g. inspections, enforcement actions, guidance issuance) systematically recorded and tracked?	1	Have initial steps been taken to explore ways to review and assess the performance of supervisory authorities based on recorded supervisory activities?	1	Are supervisory tasks evaluated across sectors through structured reviews or audits, even if limited in scope or frequency?	1	Are supervisory tasks evaluated across sectors through structured reviews or audits, even if limited in scope or frequency?	1	Are evaluation practices (e.g. feedback loops, peer reviews, cross-sectoral assessments) regularly refined to enhance the effectiveness of supervisory authorities over time?	1
	7	Have you started to identify national stakeholders and authorities relevant to	1	Is a draft or partial list of stakeholders maintained by any coordinating body or authority?	1	Is there a central inventory of stakeholders and authorities, updated	1	Is the inventory integrated with national crisis response planning and used to manage	1	Is the stakeholder landscape dynamically updated based on policy shifts, incidents or	1

		cybersecurity governance?				periodically and used for coordination and communications?		stakeholder engagement and task allocation?		innovation ecosystems to ensure full inclusion?	

14. Establish cybersecurity risk-management measures

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
14 - Establish cybersecurity risk-management measures	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have you established any general cybersecurity requirements for essential and important entities to protect their operational and service-delivery systems?	1	Are there documented sector-specific guidelines or templates for essential and important entities on implementing cybersecurity protections for operational and service-delivery systems?	1	Are cybersecurity requirements for essential and important entities formally integrated into national regulations or compliance frameworks?	1	Are cybersecurity controls for operational and service-delivery systems systematically monitored, assessed and enforced across sectors, with coordination mechanisms in place?	1	Are adaptive security models or threat-informed architectures in place to ensure the ongoing protection of operational and service-delivery systems, adjusted in near real time?	1
	2	Is there a general expectation that essential and important entities will report and respond to incidents, even if they are not fully formalised?	1	Do incident response procedures and business continuity plans exist for essential and important entities, with minimal implementation or testing?	1	Are the incident response plans of critical entities aligned with national cyber crisis-management plans?	1	Are lessons learned from past incidents integrated into improved preventive and mitigation measures nationally?	1	Are predictive analytics or simulations used to anticipate and reduce the potential impact of incidents across sectors?	1
	3	Have you formulated any high-level recommendations for essential and important entities to use state-of-the-art cybersecurity technologies and practices?	1	Do you support national initiatives that encourage the adoption of cybersecurity tools (e.g. zero-trust strategies, endpoint detection and response, and security information and event	1	Do essential and important entities take into account recognised cybersecurity frameworks that incorporate state-of-the-art measures?	1	Are essential and important entities required to align with recognised cybersecurity frameworks that incorporate state-of-the-art measures?	1	Are dynamic assessments used to continuously validate whether technologies in use by essential and important entities remain state-of-the-art in light of evolving threats?	1

				management) by essential and important entities?							
	4	Are basic risk assessment templates or models available for entities to evaluate cyber threats?	1	Do you support essential and important entities in conducting formal cyber risk assessments tailored to their sector?	1	Are risk assessments used as the basis for selecting and implementing security controls?	1	Do you conduct sector-wide risk exposure analyses and share them with essential and important entities to support harmonised responses?	1	Is there an established, data-driven approach to dynamically adjusting risk-management measures based on threat intelligence and exposure trends?	1
	5	Does the overall risk management approach consider or plan to consider the different sizes of essential and important entities in designing risk-management measures?	1	Do you tailor guidance to distinguish between requirements for SMEs and large entities in terms of expected controls?	1	Are regulatory requirements risk based and scaled according to the size and systemic relevance of each essential and important entity?	1	Are impact-based risk assessments used to prioritise regulatory focus and resource allocation to higher-risk essential and important entities?	1	Is a differentiated and predictive regulatory approach applied based on impact potential, business model evolution and entity scale?	1
	6	Are any EU or international cybersecurity standards or norms (e.g. ISO/IEC 27001, the Cybersecurity Act, open-source initiatives) referenced in national guidance without mandatory enforcement?	1	Are national regulations or procurement practices encouraging voluntary use of EU/international standards (e.g. European standardisation organisations)?	1	Do national cybersecurity audits or reports assess both the implementation of standards and the cost-effectiveness of security measures?	1	Are public–private dialogues used to adapt regulatory guidance based on industry feedback regarding feasibility and cost–benefit alignment?	1	Are regulatory frameworks continuously updated to reflect both cost-effective practices and emerging global standards?	1
	7	Are there mechanisms available for entities to self-assess and improve their own cybersecurity posture?	1	Do you recommend maturity models or gap analysis tools to essential and important entities for periodic self-evaluation?	1	Have you established a national framework to evaluate and improve the relevance and practicability of cybersecurity measures required from essential and important entities?	1	Are feedback loops in place between regulators and entities to refine practices and policies based on real-world outcomes?	1	Are forward-looking technologies (e.g. AI for risk modelling) used to inform continuous adaptation and improvement in cybersecurity measures?	1
	8	Have you proposed comprehensive non-binding recommendations for	1	Do you provide baseline guidance for the implementation of technical, operational	1	Have you established technical, operational and organisational requirements for	1	Have you established different requirements based on system sensitivity, sector or	1	Do you continuously monitor emerging technologies and evolving threat	1

		essential and important entities to comply with the risk-management requirements set out in Article 21 of NIS2?		and organisational measures by essential and important entities to comply with the risk-management requirements set out in Article 21 of NIS2?		essential and important entities in alignment with European and international standards and best practices?		threat exposure and harmonised them with requirements set up in other sectoral regulations (e.g. DORA)?		landscapes to adapt and optimise minimum cybersecurity requirements, thereby enhancing the resilience of essential and important entities against future threats?	
	9	Have you conducted consultations with representatives of essential and important entities and relevant sectoral associations to incorporate their inputs into the baseline cybersecurity requirements?	1	Have relevant stakeholders been identified and formally tasked with controlling whether baseline cybersecurity measures are properly applied by essential and important entities?	1	Do you enforce obligatory requirements for digital service providers as outlined in Commission Implementing Regulation (EU) 2024/2690 on cybersecurity risk-management measures under Directive (EU) 2022/2555?	1	Is there a process in place for regularly reviewing and updating the baseline cybersecurity measures for essential and important entities?	1	Do you actively consult with other Member States with the aim being to harmonise baseline cybersecurity measures, leverage best practice and anticipate emerging challenges?	1

15. Establish incident reporting mechanisms

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
15 – Establish incident reporting mechanisms	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have preliminary reporting procedures been drafted to support structured voluntary incident reporting under NIS2, including templates for reporting incidents, cyber threats and near misses?	1	Has a legal framework been adopted to regulate voluntary structured incident reporting, covering non-significant incidents, cyber threats and near misses?	1	Are standardised reporting templates (e.g. the non-mandatory reporting templates developed by the NIS2 Cooperation Group) available for essential and important entities to support prompt and structured mandatory incident notification?	1	Are mandatory incident-reporting mechanisms (e.g. procedures and templates) regularly evaluated and audited to improve data quality, incorporating insights from NIS2 peer reviews, best practice guides and technological developments?	1	Does the legal reporting framework include innovative mechanisms for secure tracking and verification of incident reports, enhancing transparency and reliability through lessons learned?	1
	2	Do you organise consultations with sector representatives to develop and refine reporting templates, leveraging the support and updates provided by the NIS2 Cooperation Group's working session on incident reporting?	1	Have you developed sector-specific instructions to guide entities to comply with incident-reporting requirements?	1	Have you deployed a centralised reporting platform offering standardised templates for submitting cross-border impact assessments and for essential and important entities to submit accurate and compliant incident notifications?	1	Do you regularly review and update templates and instructions based on industry feedback to improve reporting practices including cross-border reporting procedures and data quality?	1	Have you implemented advanced analytical tools (e.g. algorithms, data platforms) to improve data quality and support real-time assessment of cross-border impacts?	1
	3	Are requirements for tools to facilitate incident reporting being	1	Are there channels allowing essential and important entities and	1	Do you have a secure, centralised platform that allows entities to submit	1	Are incident reporting tools regularly evaluated and audited to improve	1	Do incident reporting tools use automated technologies, such as	1

		collected from important and essential entities?		other entities to submit information about significant incidents to competent authorities within the required time frames or under voluntary incident reporting?		incident notifications in a structured way, within the time frames established by NIS2 and providing your CSIRTs with real-time alerts for individual incidents?		data quality, incorporating insights from stakeholders (e.g. important and essential entities, CSIRTs) and best practices (e.g. from NIS2 peer reviews or guidance)?		machine learning, to refine reports submitted to CSIRTs, supporting data validation and analysis for efficient incident management and strategic response planning?	
	4	Have definitions and criteria been established to identify 'significant' incidents, including factors such as geographical spread, duration, impact severity and cross-border relevance?	1	Is there a set of clear criteria specifying thresholds for severity and scope, particularly for digital infrastructure, ICT service management and digital providers, to classify incidents as 'significant', including considerations of impact, duration and cross-border implications?	1	Have you incorporated the NIS2 definition of a 'significant' incident (i.e. any incident causing or capable of causing severe operational disruption, financial loss or considerable material or non-material damage) into your national frameworks to ensure consistent assessment and notification procedures by entities?	1	Do you regularly review threat assessments and stakeholder feedback to refine the criteria for identifying significant incidents, in line with evolving industry standards and best practices?	1	Have you used advanced data analytics technologies to continuously refine incident classification parameters and support timely, informed decision-making?	1
	5	Have you conducted initial training sessions for relevant entities to clarify responsibilities regarding mandatory and voluntary reporting of incidents?	1	Have you developed and made easily accessible guidelines to support relevant entities in meeting their reporting obligations?	1	Do you actively participate in public and sector-specific events to raise awareness among relevant entities about mandatory and voluntary incident reporting obligations?	1	Are your guidelines and training programmes regularly assessed and updated based on feedback from relevant entities?	1	Have you deployed advanced educational tools (e.g. interactive e-learning platforms) that incorporate new compliance and reporting requirements?	1
	6	Have you conducted workshops to help entities assess and flag incidents with potential cross-sectoral or cross-border impact?	1	Have you developed and made accessible practical guidelines to help relevant entities assess and report potential cross-sectoral or cross-border impacts in incident notifications?	1	Have you developed clear and consistent criteria for entities to assess and report cross-sectoral or cross-border impacts in incident notifications?	1	Do you regularly refine criteria for assessing cross-sectoral and cross-border impacts based on feedback from reporting entities?	1	Do you use advanced techniques, such as predictive analytics, to support dynamic assessments of cross-border impacts in incident reporting?	1
	7	Have you engaged in consultations with national CSIRTs and sectoral competent	1	Have national CSIRTs and sectoral authorities been formally tasked with receiving and	1	Have you implemented a centralised communication system linking CSIRTs and	1	Are the competencies of sectoral authorities regularly reviewed, and are new relevant	1	Do designated CSIRTs and competent authorities use adaptive technologies (e.g.	1

		authorities to identify the stakeholders who will be responsible for receiving and processing incident notifications and for stakeholder consultations?		processing incident notifications and providing stakeholder consultations?		sectoral competent authorities with standardised procedures for incident reporting and processing?		authorities identified to maintain an up-to-date and effective stakeholder network?		dynamic data monitoring) to improve the responsiveness to incident reports?	
	8	Have you established basic communication channels and coordination between competent authorities and CSIRTs to comply with reporting obligations under relevant legislation (e.g. the GDPR, DORA)?	1	Have procedures and standard operating protocols been adopted to set out communication responsibilities and ensure rapid, coordinated sharing of cybersecurity incident reports between CSIRTs and competent authorities?	1	Do you use standardised communication protocols and shared platforms to enable efficient, timely and structured exchange of cybersecurity incident information among competent authorities, CSIRTs and regulators?	1	Do you regularly evaluate and update communication protocols between competent authorities and CSIRTs incorporating feedback mechanisms to assess incident report quality and adapt to evolving operational and technological developments?	1	Do you use automation and real-time analytics tools to enhance rapid, efficient information exchange and incident routing between competent authorities and CSIRTs?	1
	9	Have you assessed all potential counterparts of your national single point of contact and the expected information flows to set up processes for receiving and disseminating incident information promptly and accurately?	1	Have you established and documented processes ensuring efficient information flows between the national single point of contact and other relevant stakeholders (e.g. CSIRTs, sectoral competent authorities, ENISA, the European Commission)?	1	Have structured protocols and communication platforms been implemented to ensure that the single point of contact can manage and distribute incident data accurately and in a timely manner?	1	Do you regularly review and optimise the processes and tools used by the single point of contact to improve its ability to handle and disseminate incident information?	1	Do you use predictive analytics, automation or similar technologies to enhance the single point of contact's efficiency in disseminating incident information and coordinating response efforts?	1
	10	Has the development of protocols for timely information sharing with single points of contact during cross-border or cross-sector incidents been initiated?	1	Have guidelines been developed to coordinate information flows between single points of contact during cross-border or cross-sector incidents?	1	Do you use standardised procedures and communication tools to enable the seamless exchange of incident data between single points of contact during cross-border and cross-sector incidents?	1	Do you regularly evaluate and update information-sharing protocols with the single point of contact to improve its effectiveness in cross-border and cross-sector incident coordination?	1	Do you use adaptive technologies to support real-time information sharing and collaboration, enhancing the single point of contact's ability to manage cross-sector and cross-border incidents effectively?	1

	11	Is there an ongoing initiative aimed at using aggregated incident data to enhance national situational awareness, sectoral risk assessments and strategic planning?	1	Have guidelines been developed for compiling and analysing incident data to identify trends that inform national cybersecurity planning?	1	Are data analysis and aggregation systems in place to support cross-sectoral risk assessments and inform national cybersecurity planning?	1	Are data aggregation and analysis processes regularly reviewed and optimised to align with national cybersecurity and resilience objectives?	1	Are adaptive data analytics platforms in place that use machine learning to generate real-time insights into emerging threats and support strategic decision-making?	1
	12	Are single points of contact and national authorities aware of the Cybersecurity Incident Reporting and Analysis System (CIRAS) and its capabilities for facilitating structured incident reporting and analysis?	1	Have guidelines been developed to assist relevant national entities in understanding and effectively utilising CIRAS for incident reporting?	1	Do you submit reports to CIRAS on a regular basis, at least every three months, to maintain consistent and up-to-date incident tracking?	1	Are lessons learned from past incidents integrated into future reporting and response strategies, with feedback loops established to continuously improve CIRAS utilisation?	1	Is there a data-driven regulatory approach that utilises insights from CIRAS to inform national cybersecurity policies and strategies?	1

3.1.3 Cluster #4: Regulatory and policy frameworks

16. Balance Security with Privacy

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
16 – Balance security with privacy	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have you considered incorporating the EU's regulatory measures and privacy-by-design and data protection principles into your NCSS?	1	Have steps been taken to draft guidelines, policies or strategies within your NCSS that incorporate initial measures of privacy-by-design and privacy-by-default principles using EU regulatory tools?	1	Has your NCSS incorporated EU data protection laws and applicable national data protection legislation to ensure that cybersecurity actions respect privacy rights and include safeguards such as data minimisation and access controls?	1	Do you regularly update your NCSS to reflect all of the changes to the relevant regulatory tools provided by the EU through collaborative frameworks with stakeholders to systematically implement GDPR/LED data protection principles?	1	Does the NCSS include dynamic strategies to adaptively integrate data protection principles, guided by regulatory advancements, stakeholder input and emerging threats and technologies?	1
	2	Have you considered integrating privacy-by-design, privacy-by-default and data protection principles into your cybersecurity initiatives?	1	Are initial measures to incorporate privacy-by-design and privacy-by-default principles in your cybersecurity frameworks under way, even if limited in scale?	1	Are privacy-by-design and data protection principles fully integrated into the standard operating procedures of all cybersecurity frameworks?	1	Do you conduct regular reviews of cybersecurity frameworks to ensure ongoing compliance with data protection regulations, refining processes based on emerging threats and technologies?	1	Are adaptive measures, such as real-time privacy impact assessments and automated compliance checks, implemented to continually improve privacy and data protection integration in	1

									your cybersecurity frameworks?	
	3	Does your NCSS include plans to set up coordination structures, such as joint working groups, between cybersecurity and data protection authorities?	1	Have initial frameworks been created to coordinate cybersecurity and data protection authorities in line with NIS2 and GDPR/LED requirements?	1	Are regular joint working group meetings in place within the NCSS to ensure that cybersecurity measures comply with the GDPR/LED and applicable national data protection legislation?	1	Are coordination processes between national cybersecurity authorities and data protection authorities systematically evaluated and refined within your NCSS to enhance alignment and ensure compliance with NIS2, the GDPR/LED and applicable national data protection legislation?	1	Are adaptive collaboration tools in place, such as real-time data-sharing platforms, implemented within joint working groups to continuously enhance the efficiency, responsiveness and alignment of cybersecurity and data protection initiatives?	1
	4	Have you conducted studies or analyses to identify areas for improvement in protecting citizens' privacy rights?	1	Have you identified key national stakeholders to contribute to the enhancement of the protection of citizens' privacy within cybersecurity?	1	Are structured frameworks in place within your NCSS to ensure that privacy is consistently prioritised across all cybersecurity measures and activities?	1	Do you regularly assess and optimise frameworks to ensure the consistent prioritisation of privacy within national cybersecurity efforts?	1	Are technical and organisational measures (e.g. encrypted logging, anonymised threat intelligence sharing, privacy-compliant monitoring) systematically promoted and integrated into cybersecurity practices and frameworks?	1
	5	Is there an initial effort under way to develop guidance or frameworks to support the implementation of privacy-respectful cybersecurity solutions?	1	Have you piloted any national-level guidance or frameworks to support privacy-compliant cybersecurity implementation?	1	Are national-level guidance documents and frameworks actively published and disseminated to support privacy-compliant cybersecurity implementation?	1	Is there an established process to systematically integrate lessons learned from domestic and international privacy-focused cybersecurity initiatives into national frameworks?	1	Is your country positioning itself as a leader in EU forums and discussions on good practices in developing and distributing guidance supporting GDPR-/LED-compliant cybersecurity solutions?	1
	6	Have you considered the importance of adopting technical and organisational measures that address the balance between privacy and	1	Have you started to promote policies that encourage public and private entities to adopt technical and organisational measures that align with EU privacy and cybersecurity requirements such as	1	Are technical and organisational measures actively adopted to meet both privacy and cybersecurity standards (e.g. anonymised threat intelligence sharing)?	1	Are certifications (e.g. ISO/IEC 27701:2019) promoted within a formal cross-sectoral framework that incorporates performance monitoring	1	Are innovative solutions, such as real-time data protection and adaptive compliance monitoring, employed to continuously optimise the balance between	1

		cybersecurity requirements?		encryption and privacy-compliant monitoring?				and regular feedback loops?		privacy and cybersecurity?	
	7	Have you discussed with relevant stakeholders (e.g. law enforcement agencies, data protection agencies) the incorporation of data protection impact assessments (DPIAs) as a standard practice for assessing data protection risks in cybersecurity initiatives?	1	Have initial requirements been established to conduct DPIAs for evaluating personal data processing risks within cybersecurity policies?	1	Have you incorporated the DPIAs as an integral part of the NCSS development process, ensuring compliance and risk mitigation in data handling?	1	Are DPIA practices regularly reviewed and enhanced through stakeholder consultations to ensure alignment with current data protection requirements?	1	Are adaptive technologies deployed to support DPIA processes and enhance their effectiveness in managing evolving personal data protection risks?	1
	8	Have initial oversight mechanisms been considered to assess the impact of national cybersecurity practices and legal frameworks on privacy and data protection?	1	Has a responsible stakeholder been designated to oversee and assess the impact of national cybersecurity practices and legal frameworks on privacy and data protection?	1	Are oversight mechanisms established and functioning to regularly assess and address the impact of national cybersecurity practices and legal frameworks on privacy and data protection?	1	Are sector-specific cybersecurity policies and standards systematically reviewed and updated to ensure the integration of privacy and data protection considerations, incorporating stakeholders' feedback and best practices?	1	Do you have mechanisms in place to monitor the latest technological developments in order to adapt relevant privacy and data protection guidelines and legal obligations?	1
	9	Have you taken initial steps to support R & D or the adoption of privacy-enhancing technologies (PETs), such as anonymisation techniques and secure multi-party computation in the public and private sectors?	1	Have you identified key national stakeholders for R & D efforts on the topic of PETs?	1	Are policies in place for the adoption of PETs for public and private sectors?	1	Are PET initiatives continuously evaluated, incorporating stakeholders' feedback to improve and support frameworks and adoption?	1	Is the participation in and the promotion of PET R & D driven by continuous innovation, leveraging emerging technologies and strategic foresight to anticipate future needs and proactively advance solutions?	1
	10	Is there an initial plan to introduce	1	Have initial strategies been developed to incorporate	1	Are privacy and data protection	1	Are sector-specific cybersecurity policies	1	Are advanced technologies, such as	1

		preliminary privacy-focused frameworks into cybersecurity policies for sectors handling sensitive personal data, such as health, finance and identity data?		privacy and data protection measures into cybersecurity standards for sectors managing particularly sensitive personal data (special categories of data per the GDPR), in alignment with the GDPR/LED and applicable national legislation?		considerations fully integrated into sector-specific cybersecurity policies to ensure consistent embedding across cybersecurity measures?		regularly reviewed and optimised, incorporating audits and stakeholder feedback loops, to ensure effective integration of privacy and data protection?		adaptive solutions with real-time monitoring, deployed to enhance privacy and data protection integration across sector-specific cybersecurity initiatives?	

17. Improve the Cybersecurity of the Supply Chain

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
17 – Improve the cybersecurity of the supply chain	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Do you have any informal or formal plans to evaluate supplier risk and consider criteria for the assessment of critical and high-risk ICT suppliers?	1	Have you developed an initial framework or draft criteria to assess the risk profile of ICT suppliers, including geopolitical, legal, sector-specific and cybersecurity-related factors?	1	Have you performed a national-level risk assessment (services, technologies and products) based on a formal framework for evaluating high-risk suppliers, and are essential and important entities required to assess suppliers accordingly, with national guidance and oversight in place?	1	Is the supplier risk assessment framework regularly updated and used in national procurement policies and regulations to restrict or exclude high-risk suppliers from critical ICT supply chains, based on national and EU-coordinated risk assessments?	1	Do you proactively use real-time intelligence, EU warnings and emerging threat indicators to adapt the supplier evaluation framework, enforce responsive restrictions and mandate cybersecurity-related procurement requirements to mitigate evolving supply chain risks?	1
	2	Have you begun to assess strategic dependencies in ICT supply chains or explored the feasibility of developing a national-level multi-vendor strategy?	1	Have you created initial policies or frameworks to support multi-vendor strategies and considered thresholds for supplier diversification based on factors such as market share or geopolitical risks?	1	Are policies on strategic dependency and supplier diversification formally adopted and supported by operational mechanisms (e.g. thresholds, criteria or incentives), and are critical entities engaged	1	Have you institutionalised regular reviews of supplier diversification and strategic dependency risks, including applying specific thresholds (e.g. > 50 % market share or geopolitical exposure) and established	1	Do you dynamically monitor and respond to strategic dependency risks by adapting supplier diversification policies (e.g. nearshoring, dual sourcing), promoting multi-vendor resilience across entities and	1

					in applying these measures?		collaboration with entities for implementing mitigation strategies?		incentivising innovation and redundancy?	
	3	Have you performed a study on cybersecurity good practices for supply chain management that is used by procurement in various industry segments and/or in the public sector?	1	Are initial guidelines or draft baseline security requirements for supply chains under development based on European or international standards?	1	Have you published national guidance for supply chain security?	1	Are supply chain security requirements embedded across sectors and harmonised with EU-wide and international standards (e.g. ISO/IEC 27001)?	1	Do you actively contribute to and align with international and EU efforts on supply chain cyber resilience?	1
	4	Have you informally or officially acknowledged the importance of ensuring that critical suppliers implement supply chain risk measures?	1	Do you encourage/enforce any requirements, pilots or sectoral efforts to promote baseline cybersecurity measures for critical suppliers?	1	Do you have national requirements or incentives for critical suppliers to apply cybersecurity risk measures?	1	Are supplier compliance and effectiveness monitored systematically through audits and reports?	1	Is the implementation of risk measures by suppliers regularly reviewed and adjusted based on evolving threats and sector needs?	1
	5	Have you identified the need for public guidance on supply chain risk management for SMEs?	1	Are initial public guidance materials or awareness campaigns targeting SMEs being developed or disseminated?	1	Is there comprehensive, regularly updated public guidance tailored to SMEs on managing supply chain cybersecurity risks?	1	Is public guidance for SMEs co-developed or validated with stakeholders and linked to sector-specific or EU-level guidance?	1	Is public guidance for SMEs continuously refined based on emerging risks, SMEs' feedback and lessons learned from incidents and audits?	1
	6							Do you actively participate in the design and implementation of the EU cybersecurity certification framework and the development and/or maintenance of EU cybersecurity certification schemes for ICT digital products, services and processes, as established in the Cybersecurity Act (e.g. participation in the European Cybersecurity Certification Group,	1		1

							promotion of technical standards and procedures for ICT product/service security)?			
	7	Have you initiated discussions on identified ICT supply chain risks at EU-level forums?	1	Have you engaged relevant stakeholders at EU-level forums in ICT supply chain risk assessment through shared lessons learned?	1	Is there structured cooperation and data sharing across agencies and national mechanisms (e.g. covering cybersecurity, procurement and critical infrastructure) to coordinate risk assessments and ICT supply chain incident collection and analysis, in line with Article 29 of NIS2?	1	Do you contribute to EU-level risk assessments to promote inter-agency and cross-sector collaboration on ICT supply chain security?	1	Have you established continuous collaboration with EU-level forums and programmes to strengthen ICT supply chain risk mitigation and awareness?	1
	8	Have you recognised the need for secure ICT supply chains and begun identifying ways to include cybersecurity in public procurement processes?	1	Have you started adding basic cybersecurity requirements to ICT procurement processes and engaged with EU supply chain initiatives?	1	Do you consistently apply cybersecurity rules in procurement processes, support SMEs in doing so and cooperate with EU programmes in order to achieve them?	1	Have you aligned national procurement policies with EU recommendations and promoted secure solutions across all sectors?	1	Do you lead or co-lead EU-wide initiatives to strengthen supply chain security, drive innovation and update strategies based on new threats?	1
	9	Have you acknowledged the relevance of standards, certification and secure-by-design principles for ICT supply chain security and begun identifying relevant forums and stakeholders?	1	Have you started participating in standardisation and certification activities at the EU or international levels, and initiated coordination efforts among market surveillance, industry and researchers on vulnerability discussions?	1	Do you ensure regular representation in relevant standardisation and certification bodies, integrate vulnerability information into national supply chain risk processes and promote open standards and secure-by-design practices across sectors?	1	Have you established formal mechanisms to maintain and contribute to certification schemes and vulnerability assessments, while supporting multistakeholder collaboration to apply open standards and ensure coherence with EU frameworks?	1	Do you lead or co-lead initiatives to shape international certification and standards policies, proactively coordinate vulnerability information sharing between stakeholders or foster innovation in secure-by-design practices, promoting them as a national norm for ICT procurement and supply chain resilience?	1

	10							Is there a national directory of critical suppliers used to inform policy decisions, risk assessments and incident response coordination?	1	Is the directory dynamically maintained using real-time updates, stakeholder inputs and threat intelligence feeds?	1
	11	Do you plan or pilot structured testing activities (e.g. stress testing, sandboxes) specifically targeting critical sectors or suppliers?	1	Do you perform structured testing (e.g. stress testing, sandboxes) to validate the resilience and security of supply chain and ICT products/services?	1	Do you have national frameworks that regularly conduct structured testing activities (e.g. stress testing, sandboxes) with relevant entities and document lessons learned?	1	Do you integrate testing (e.g. stress testing, sandboxes) into the procurement, certification or operational life cycle of critical systems and test results into national preparedness plans and supply chain policies?	1	Do you continuously improve the structured testing activities (e.g. stress testing, sandboxes) based on feedback, simulations, emerging risks and international collaboration?	1

18. Protect Critical Sectors

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
18 – Protect critical sectors	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have initial steps been taken to establish an inventory and classification system for essential and important entities and critical assets in line with Annexes I and II to NIS2 (e.g. identifying additional sectors and defining classification or setting up a registration mechanism)?	1	Has a comprehensive inventory and classification of essential and important entities and critical assets been completed to identify those that have a significant impact on national security and public safety?	1	Is global governance (stakeholders' roles and responsibilities) clearly established to ensure the consistent application of protective measures across essential and important entities and high-priority assets?	1	Are there any established mechanisms to regularly update and refine the inventory and classification system, ensuring that it stays aligned with national security needs and priorities?	1	Does the classification framework incorporate emerging data analytics and technologies to enhance the understanding and protection of essential and important entities and critical assets?	1
	2	Have you started the creation of collaborative platforms between competent authorities and private sector operators, laying the foundation for formal cooperation?	1	Are there collaborative mechanisms in place, such as PPPs and working groups on critical information infrastructure protection, to engage stakeholders?	1	Are these collaborative platforms operational, with active participation from both competent authorities and private entities to enhance security efforts within essential and important entities?	1	Is there regular evaluation and improvement of these collaborative mechanisms to ensure that they effectively address the shared security needs of essential and important entities?	1	Do these collaborative structures employ advanced communication tools and strategies to proactively manage risks, leveraging real-time data and insights for increased resilience?	1

	3	Have you identified the unique security needs of essential and important entities as defined in Annexes I and II to NIS2?	1	Have sector-specific policies and guidelines been developed to ensure the availability, integrity and confidentiality of services in essential and important entities?	1	Have sector-specific security policies, baselines and guidelines been implemented across essential and important entities, with monitoring and governance in place?	1	Are sector-specific security policies and baselines regularly reviewed and updated to address evolving cybersecurity needs and risks?	1	Do you use foresight methodologies such as predictive analytics and threat intelligence to regularly update sector-specific security policies, anticipating emerging risks and technological changes?	1
	4	Is there informal or official recognition within your NCSS of the importance of protecting undersea communications cables as critical components of global digital infrastructure and connectivity?	0	Have specific action plans been established to address the cybersecurity needs of undersea communications cables, in line with sector-specific guidelines?	0	Are protective measures for undersea communications cables implemented and integrated into broader digital resilience strategies?	0	Are cross-sector collaboration frameworks in place (e.g. involving digital infrastructure, transport and public administration) to support regular reviews of and joint efforts to protect undersea communications cables as essential components of global connectivity?	0	Are comprehensive strategies in place that leverage global insights and best practices to continuously adapt and enhance cybersecurity measures for the public core of the internet, particularly undersea communications cables?	0
	5	Has the protection of foundational internet infrastructure (e.g. the domain name system, border gateway protocol routing, internet exchange points and time synchronisation services) been incorporated into the NCSS?	1	Have specific measures been established to protect foundational internet infrastructure through coordinated efforts involving relevant sectors and cross-border cooperation?	1	Are comprehensive protective measures for foundational infrastructure elements developed and systematically implemented across relevant sectors, supported by governance frameworks coordinating cybersecurity and physical resilience efforts?	1	Are performance monitoring mechanisms in place to regularly assess and update protection strategies for foundational internet infrastructure?	1	Are predictive analytics and collaborative platforms used to dynamically refine protection measures for foundational internet infrastructure, fostering proactive resilience strategies against emerging threats?	1

19. Establish a CVD Policy

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
19 – Establish a Coordinated Vulnerability Disclosure (CVD) policy	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Have you taken the first steps to establish a national CVD policy and supporting framework?	1	Does your national CVD approach designate a coordinating authority (e.g. a CSIRT) and establish its role and responsibilities as regards vulnerability reports?	1	Does your national CVD policy include a structured process for reporting vulnerabilities, provide mechanisms for disclosure (including anonymous options) and specify timelines for response and remediation that balance urgency, transparency and cybersecurity?	1	Has your national CVD implementation included awareness campaigns to reach NIS2 entities and/or incentives to foster collaboration among stakeholders and researchers?	1	Are processes in place to adapt the national CVD policy to emerging threats and legislative changes?	1
	2	Do you recognise the need to adopt protective measures to prevent the prosecution of cybersecurity researchers acting in good faith?	1	Have you published guidelines for cybersecurity researchers, including acceptable and unacceptable vulnerability discovery methods?	1	Does your national CVD policy include provisions for limited liability or 'safe harbour' for cybersecurity researchers acting in good faith?	1	Do you regularly review and improve protective measures or guidelines that prevent the prosecution of cybersecurity researchers in order to optimise their effectiveness?	1	Are there processes in place to predict and address upcoming legal implications (stemming from new regulations or new technologies) affecting cybersecurity researchers and CVD policies?	1
	3	Have you identified suitable technical tools for secure and trusted	1	Do you provide guidelines for submitting vulnerability reports in a trusted and secure way	1	Have you adopted tools (e.g. dedicated secure portals, validation systems) to facilitate	1	Have you implemented feedback mechanisms to improve the cybersecurity and	1	Do you regularly monitor the latest technology advancements and assess how they could	1

		handling of vulnerability reports?		(e.g. through a specific portal)?		trusted and secure vulnerability disclosure with adequate anonymity and data protection mechanisms?		reliability of tools used for handling vulnerability reports?		contribute to improving your CVD tools and processes?	
	4	Have you framed general conditions to promote safe and responsible vulnerability research?	1	Do you promote the adoption of CVD policies or bug bounty programmes by essential and important entities?	1	Do you offer incentives (e.g. financial rewards, recognition) to encourage cybersecurity researchers to participate in CVD activities?	1	Do you promote CVD practices among public and private researchers with the support of research programmes (e.g. Horizon Europe, the digital Europe programme)?	1	Have you participated in international or EU-level initiatives to encourage cybersecurity researchers to engage in CVD programmes (e.g. the European Commission's free and open-source software auditing project)?	1
	5	Are you planning to actively consult with the European Vulnerability Database?	1	Do you encourage private sector entities (e.g. suppliers of network and information systems or manufacturers) and cybersecurity researchers to share information in the European Vulnerability Database?	1	Does your competent authority or team (e.g. your CSIRT) actively contribute to the European Vulnerability Database?	1	Does your competent authority or team (e.g. your CSIRT) actively cooperate with other Member States' competent authorities or teams on CVD through official EU channels (e.g. the CSIRTs Network)?	1	Do you actively support or lead a broader dialogue in EU and international forums (e.g. the CSIRTs Network, the NIS2 Cooperation Group) on vulnerability handling and management good practices and/or share and improve protective measures for cybersecurity researchers?	1

20. Promote Active Cyber Protection

NCSS objective	#	Level 1	R	Level 2	R	Level 3	R	Level 4	R	Level 5	R
20 – Promote active cyber protection	a	Do you cover the objective in your NCSS or do you plan to cover it in the next edition?	1	Have you defined (formally or informally) intended results, guiding principles, or key activities in your action plan that contribute to achieving the objective in an uncoordinated way?	1	Do you have a formally defined and documented action plan that includes specific activities with clear goals, timelines, and allocated resources?	1	Do you have a formal mechanism to regularly review and assess your action plan to ensure that it is correctly prioritized and optimized, including progress tracking, performance evaluation, and identification of areas for improvement?	1	Do you have mechanisms in place to ensure that the action plan is monitored and dynamically adapted to evolving technological, geopolitical and threat landscapes?	1
	1	Are there unofficial or formal efforts to promote ACP as part of a broader defensive strategy?	1	Have you identified key stakeholders from the public and private sectors and civil society to be involved in or benefit from ACP under your NCSS?	1	Have ACP policies been adopted under your NCSS and integrated into a broader national defensive strategy?	1	Are ACP policies regularly evaluated and optimised to ensure alignment with a broader national defensive strategy?	1	Are ACP policies continuously updated to address emerging threats and cybersecurity trends and integrated into the broader national defensive strategy?	1
	2	Do you recognise the need for sectoral security operations centres (SOCs) to enhance threat detection and incident response capabilities across critical sectors in your country?	1	Do you have any policy on establishing sectoral SOC to support entities across your country?	1	Have you established operational sectoral SOCs with clear roles and responsibilities and secure communication channels for sharing threat intelligence among essential and important entities?	1	Do your sectoral SOCs actively exchange threat intelligence information with other national stakeholders (e.g. national CSIRTs) to improve awareness and incident response?	1	Do you promote threat information sharing and good practice sharing between SOCs, enabling cross-sector and cross-border collaboration?	1
	3	Do key public administration entities implement basic monitoring/alerting capabilities (e.g. logs, basic intrusion	1	Are safeguards in place to support informed and responsible implementation and use of ACP?	1	Are real-time detection/monitoring capabilities (e.g. intrusion detection systems, security information and event management, SOCs)	1	Is information sharing tailored to the cyber posture and the size/type of stakeholders (e.g. SMEs, large entities, public administration entities) to ensure	1	Are analytics and detections dynamically adjusted using intelligence-driven models and continuous purple-team exercises to proactively anticipate	1

		detection systems) for critical networks?				operational across critical sectors, supported by clear incident response playbooks?		relevance and avoid information overload?		and respond to emerging cyber threats?	
	4	Are there awareness-raising initiatives to inform stakeholders about the benefits and use of ACP tools and services?	1	Have you identified target entities to offer free ACP tools and services (e.g. self-service checks, detection tools, takedown services)?	1	Is there a national programme for identifying, acquiring, customising and operating ACP tools and services and making them available to relevant stakeholders?	1	Are mechanisms in place to ensure that ACP tools and services are regularly updated and optimised in response to operational feedback?	1	Is there a mechanism for continuously integrating novel or emerging ACP tools and services, including enhanced threat intelligence sharing, into routine cybersecurity operations across sectors?	1
	5	Are formal or informal procedures and communication channels (e.g. mailing lists, ad hoc alerts) in place to facilitate threat intelligence sharing among public and private stakeholders?	1	Are formal mechanisms being developed or piloted to support structured and trusted threat intelligence exchange among stakeholders?	1	Is a national threat intelligence platform (e.g. an MISP or OpenCTI platform) operational and used by key stakeholders to enable unified and structured information sharing?	1	Are threat intelligence sharing procedures and arrangements regularly assessed, updated and optimised based on stakeholder feedback and operational needs?	1	Have national initiatives been launched to foster communities of trust among stakeholders and to promote voluntary, secure and optionally anonymous threat intelligence sharing (e.g. anonymous sharing platforms)?	1

3.2 Guidelines to use the framework

This section provides Member States some guidelines and recommendations for rolling out the framework and for filling out the questionnaire:

Anticipate coordination activities to gather and consolidate data. Most Member States indicate that completing a self-assessment typically requires around 15 person-days. Conducting the assessment involves engaging a wide range of stakeholders. It is therefore recommended to allocate sufficient time during the preparation phase to identify all relevant stakeholders across government bodies, public agencies, and the private sector.

Identify a central body in charge of completing the self-assessment at national level. Since gathering material for NCAF 2.0 indicators might involve numerous stakeholders, it is recommended to establish a central body or agency responsible for coordinating with and liaising among all relevant stakeholders to complete the self-assessment.

Use the assessment exercise as a way to share and communicate on cybersecurity topics. Lessons learnt from Member States indicate that discussions, whether through individual interviews or collective workshops, provide a valuable forum to foster dialogue, share perspectives and identify areas of improvement. In addition to highlighting key achievements, sharing results can help raise awareness and promote cybersecurity initiatives.

Use the NCSS to define the scope of the objectives for assessment. The 20 objectives in NCAF 2.0 were derived from the objectives commonly addressed by Member States in their NCSS. While the NCSS can guide which objectives to include, it should not limit the assessment. Since the NCSS naturally prioritises certain areas, some objectives may be omitted, but this does not imply that the corresponding capacities are absent. For example, if a specific objective is not included in the NCSS but the country has related cybersecurity capabilities, that objective can still be assessed.

When the NCSS scope evolves, ensure that the score interpretation remains consistent with these changes. The NCSS lifecycle spans multiple years, with many Member States implementing 3 to 5-year roadmaps that may include changes in scope between successive editions. Consequently, special care is needed when comparing self-assessment results across NCSS editions, as scope changes can affect the final maturity score. It is recommended to compare scores across the full set of strategic objectives from one year to the next (i.e., the 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 2.5 on the scoring mechanism), the overall specific coverage ratio is equal to or higher than the overall general coverage ratio. This is because the overall general coverage ratio may include objectives not yet addressed by the Member State, which can lower the ratio. When a Member State adds a new objective, the overall coverage ratio will increase

(i.e., more maturity indicators are covered), while the overall specific maturity may decrease if the newly added objective is at an early stage and therefore has a low maturity level.

- When filling out the self-assessment questionnaire, remember that the primary purpose is to support Member States in cybersecurity capacity-building. Even if it is sometimes difficult to provide a definite answer, it is recommended to select the response that is most generally accepted. For example, if a question is answered YES for one scope but NO for another, the NO response indicates that action is required—either a remediation plan or a plan to address the improvement area in future developments.

SECTION 4

Annex A – Desk research bibliography

Annex A – Desk research bibliography

A.1 European Commission documents

Official Journal of the European Union (2022) DIRECTIVE (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557&qid=1749128838444

Official Journal of the European Union (2022) DIRECTIVE (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Official Journal of the European Union (2016) DIRECTIVE (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148&qid=1749128737957

Official Journal of the European Union (2024) REGULATION (EU) 2024/2847 of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847&qid=1751962706527

Official Journal of the European Union (2022) REGULATION (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2554&qid=1751972468415

Official Journal of the European Union (2021) REGULATION (EU) 2021/887 of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887&qid=1751962872176

Official Journal of the European Union (2019) REGULATION (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881&qid=1751963273613

Official Journal of the European Union (2024) COMMISSION RECOMMENDATION (EU) 2024/1101 of 11 April 2024 on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C%282024%297151

Official Journal of the European Union (2024) COMMISSION IMPLEMENTING REGULATION (EU) C/2024/7151 final of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regards to “various providers”. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=intcom:C%282024%297151

European Commission (2023) COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL COM (2023) 207 final of 18 April 2023 – Closing the cybersecurity talent gap to boost the EU’s competitiveness, growth and resilience (“The Cybersecurity Skills Academy”. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/95048

European Commission (2020) JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL JOIN (2020) 18 final of 16 December 2020 – The EU’s Cybersecurity Strategy for the Digital Decade. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/72164

European Commission - NIS Cooperation Group (2020) CG Publication 01/2020 - Cybersecurity of 5G networks EU toolbox of risk mitigating measures. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468

European Network and Information Security Agency (2025) Technical Implementation Guidance: On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures. Available at: https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

European Network and Information Security Agency (2025) Handbook for Cyber Stress Tests. Available at: https://www.enisa.europa.eu/publications/handbook-for-cyber-stress-tests

European Network and Information Security Agency (2023) Building Effective Governance Frameworks for the implementation of National Cybersecurity Strategies. Available at: https://www.enisa.europa.eu/publications/building-effective-governance-frameworks-for-the-implementation-of-national-cybersecurity-strategies

European Network and Information Security Agency (2023) Undersea Cables – What is at Stake? Available at: https://www.enisa.europa.eu/publications/undersea-cables

European Network and Information Security Agency (2020) National Capabilities Assessment Framework. Available at: https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

European Network and Information Security Agency (2018) Information Sharing and Analysis Centres (ISACs): Cooperative models. Available at: https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

European Network and Information Security Agency (2016) NCSS good practice guide: designing and implementing national cyber security strategies. Available at: https://www.enisa.europa.eu/publications/ncss-good-practice-guide

European Network and Information Security Agency (2014) Report on Cyber Crisis Cooperation and Management: Comparative study on the cyber crisis management and the general crisis management. Available at: https://www.enisa.europa.eu/publications/ccc-study

European Network and Information Security Agency (2011) Cooperative Models for Effective Public Private Partnerships: Desktop Research Report Available at: https://www.enisa.europa.eu/publications/copy_of_desktop-reserach-on-public-private-partnerships

A.2 NCSS and related documents of Member States

Federal Chancellery of the Republic of Austria (2021) Austrian Cyber Security Strategy. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/AT_NCSS_2021_en.pdf

Federal Ministry of the Interior (Austria) (2024) Austrian Security Strategy. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/AT_SECURITY_STRATEGY_2024_en.pdf

Federal Ministry of the Interior (Austria) (2024) Maßnahmenkatalog der Österreichischen Strategie für Cybersicherheit 2021: Fortschrittsbericht 2/2024. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/AT_MEASURES_CATALOGUE_2024_de.pdf

Centre for Cybersecurity Belgium (2021) CYBERSECURITY STRATEGY BELGIUM 2.0 2021-2025. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/BE_NCSS_2021_en.pdf

Centre for Cybersecurity Belgium (2024) ACTIVE CYBER PROTECTION (ACP). Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/BE_POLICY_DOCUMENT_2024_en.pdf

Government of Bulgaria (2021) Updated National Cybersecurity Strategy: “Cyber-Resistant Bulgaria 2023”. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/BG_NCSS_2021_en%20%28draft%20translation%29.pdf

Government of Croatia (2022) Annual Report 2023 - NACIONALNOG VIJEĆA ZA KIBERNETIČKU SIGURNOST. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/HR_ANNUAL_REPORT_2023_hr.pdf

Government of Croatia (2023) Action Plan 2023 - IZVJEŠĆE O PROVEDBI AKCIJSKOG PLANA ZA PROVEDBU NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI 2022. Available at: https://www.uvns.hr/UserDocsImages/dokumenti/informacijska-sigurnost/Izvje%C5%A1%C4%87e%20o%20provedbi%20mjera%20Akcijskog%20plana%20NSKS%20u%202022..pdf?vel=997919

Deputy Ministry of Research, Innovation and Digital Policy of Cyprus (2020) Cybersecurity Strategy of the Republic of Cyprus 2020. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/CY_NCSS_2020_en.pdf

National Cyber Security Centre (2021) National Cyber Security Strategy of the Czech Republic. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/CZ_NCSS_2021_en.pdf

National Cyber Security Centre (2021) Action Plan for the National Cyber Security Strategy of the Czech Republic from 2021 to 2025. Available at: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/akcni_plan_2021-2025.pdf

National Cyber Security Centre (2021) 2021 REPORT ON CYBER SECURITY IN THE CZECH REPUBLIC. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/2021%20Report%20on%20Cyber%20Security%20in%20the%20Czech%20Republic_en.pdf

National Cyber Security Centre (2022) 2022 REPORT ON THE STATE OF CYBERSECURITY IN THE CZECH REPUBLIC. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/2022_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic_en.pdf

National Cyber Security Centre (2023) 2023 Report on the State of Cybersecurity in the Czech Republic. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/2023_Report_on_the_State_of_Cybersecurity_in_the_Czech_Republic_en.pdf

The Danish Government (2021) The Danish National Strategy for Cyber and Information Security 2022. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/DK_NCSS_2022_en.pdf

Republic of Estonia, Ministry of Economic Affairs and Communications (2024) CYBERSECURITY STRATEGY 2024–2030 ‘CYBER-CONSCIOUS ESTONIA’. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EE_NCSS_2024_en.pdf

Republic of Estonia, Information System Authority (2024) CYBER SECURITY IN ESTONIA 2024’. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/EE_REPORT_ON_CYBER_SECURITY_2024_en.pdf

Prime Minister’s Office of Finland (2024) Finland’s Cyber Security Strategy 2024-2035. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FI_NCSS_2024_en.pdf

Prime Minister’s Office of Finland (2024) Implementation plan for Finland's Cyber Security Strategy 2024-2035. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/action-plans/FI_ACTION_PLAN_2024_en.pdf

National Cyber Security Centre Finland (2022) Strengthening cyber security at Finnish organisations: Instructions for management and experts. Available at: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Strengthening%20cyber%20security%20at%20Finnish%20organisations%20-%20Instructions%20for%20management%20and%20experts.pdf

République Française (2025) Plan stratégique de l’Agence nationale de la sécurité des systèmes d’information 2025-2027. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/FR_NCSS_2025_fr.pdf

Government of France (2023) National Cybersecurity Strategy, France 2030. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/FR_NCSS_PRESENTATION_2023_en.pdf

République Française (2022) National strategic review. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/FR_STRATEGIC_REVIEW_2022_en.pdf

Federal Ministry of the Interior (2021) Cyber Security Strategy for Germany 2021. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/DE_NCSS_2021_en.pdf

Hellenic Republic, Ministry of Digital Governance, National Cybersecurity Authority (2020) National Cyber Security Strategy 2020-2025. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/EL_NCSS_2020_en.pdf

Hellenic Republic, Ministry of Digital Governance, National Cybersecurity Authority (2021) Cybersecurity Handbook: Best Practices for the Protection and Resilience of Network and Information Systems. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/EL_CYBERSECURITY_HANDBOOK_en.pdf

Government of Hungary (2025) National Cybersecurity Strategy of Hungary. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/HU_NCSS_2025_hu.pdf

Government of Hungary (2024) Act on Cybersecurity in Hungary. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/HU_ACT_ON_CYBERSECURITY_2024_hu.pdf

Government of Italy (2022) National Cybersecurity Strategy 2022-2026. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/IT_NCSS_2022_en.pdf

Government of Italy (2022) Implementation Plan: National Cybersecurity Strategy 2022-2026. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/IT_IMPLEMENTATION_PLAN_2022_en.pdf

Agenzia per la Cybersicurezza Nazionale (2023) Monitoraggio della Strategia di Cybersecurity Governance: Introduzione. Available at: https://www.acn.gov.it/portale/w/monitoraggio-della-strategia-di-cybersecurity-governance-introduzione

Government of Ireland (2019) National Cyber Security Strategy 2019-2024. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/IE_NCSS_2019_en.pdf

Government of Ireland (2023) National Cyber Security Strategy 2019-2024 Mid-Term Review. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/IE_NCSS_MID_TERM_REVIEW_2023_en.pdf

Government of Latvia (2023) The Cybersecurity Strategy of Latvia 2023-2026. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LV_NCSS_2023_en.pdf

National Cybersecurity Unit, Principality of Liechtenstein (2025) National Strategy for Protection Against Cyber Risks. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LI_NCSS_2025_en.pdf

Government of Liechtenstein (2025) Cyber Security Act 2025 - Cyber-Sicherheitsgesetz (CSG). Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LI_CYBER_SECURITY_ACT_2025_de.pdf

Government of Liechtenstein (2025) Cyber Security Regulation 2025 – Cyber-Sicherheitsverordnung (CSV). Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LI_CYBER_SECURITY_REGULATION_2025_en.pdf

Government of Lithuania (2024) Progress Measure Description - 2023–2030 METŲ PLĖTROS PROGRAMOS VALDYTOJOS LIETUVOS RESPUBLIKOS, PROGRAMOS PAŽANGOS PRIEMONĖS NR. 06-007-10-05-07 „STIPRINTI KIBERNETINĮ ATSPARUMĄ“ APRAŠAS. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LT_PROGRESS_MEASURE_DESCRITPION_lt.pdf

Government of Lithuania (2024) Cybersecurity Programme Justification - 2023–2030 METŲ PLĖTROS PROGRAMOS VALDYTOJOS LIETUVOS RESPUBLIKOS - Nacionalinio pažangos plano (toliau – NPP). Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LT_CYBERSECURITY_PROGRAMME_JUSTIFICATION_lt.pdf

Government of Lithuania (2021) National Progress Plan - 2021–2030 METŲ NACIONALINIS PAŽANGOS PLANAS. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LT_NATIONAL_PROGRESS_PLAN_2021_lt.pdf

Government of Lithuania (2024) Law on Cybersecurity - LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMAS. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LT_LAW_ON_CYBERSECURITY_lt.pdf

Government of Lithuania (2021) National Cybersecurity Strategy. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/LT_SECURITY_STRATEGY_2021_lt.pdf

Government of Luxembourg (2021) National Cybersecurity Strategy IV. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/LU_NCSS_2021_en.pdf

Government of Malta (2023) National Cyber Security Strategy 2023-2026. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/MT_NCSS_2023_en.pdf

Government of Netherlands (2022) Netherlands Cybersecurity Strategy 2022-2028. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/NL_NCSS_2022_en.pdf

Government of Netherlands (2022) Action plan: Netherlands Cybersecurity Strategy 2022-2028. Available at: https://english.nctv.nl/binaries/nctv-en/documenten/publications/2022/12/06/the-netherlands-cybersecurity-strategy---action-plan/NCTV+%E2%80%A2+Actieplan+NCSS+22-28+%E2%80%A2+handreiking+EN+RGB+HR.pdf

National Coordinator for Counterterrorism and Security, Ministry of Justice and Security (2024) Cybersecurity Assessment Netherlands 2024. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/NL_ASSESSMENT_2024_en.pdf

Ministry of Digital Affairs of Poland (2019) Cybersecurity Strategy of the Republic of Poland for 2019 – 2024. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PL_NCSS_2019_en.pdf

Government of Poland (2020) National Security Strategy of the Republic of Poland. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/PL_SECURITY_STRATEGY_2020_en.pdf

Government of Portugal (2019) National Strategy for Cyberspace Security 2019-2023. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/PT_NCSS_2019_en.pdf

Government of Portugal (2022) Estratégia Nacional de Segurança do Ciberespaço 2019-2023 – Implementation report. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/PT_NCSS_IMPLEMENTATION_REPORT_2022_pt.pdf

Government of Romania (2022) NCSS - Strategiei de securitate cibernetică a României, pentru perioada 2022—2027. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/RO_NCSS_2022_ro.pdf

National Security Authority of Slovakia (2021) The National Cybersecurity Strategy 2021-2025. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/SK_NCSS_2021_en.pdf

National Security Authority of Slovakia (2021) Security Strategy of the Slovak Republic. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/SK_SECURITY_STRATEGY_2021_en.pdf

National Security Authority of Slovakia (2021) Akčný plán realizácie: Národná Stratégia Kybernetickej Bezpečnosti 2021 – 2025. Available at: https://www.nbu.gov.sk/data/att/2760.pdf

National Security Authority of Slovakia (2021) Odpočet Implementácie Akčného Plánu realizácie Národnej stratégie kybernetickej bezpečnosti na roky 2021 až 2025. Available at: https://www.nbu.gov.sk/data/att/398.pdf

Government of Spain (2019) National Cybersecurity Strategy. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/ES_NCSS_2019_en.pdf

The Federal Council (Confédération Suisse) (2023) National Cyberstrategy (NCS). Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/CH_NCSS_2023_en.pdf

Government of Sweden (2025) NCSS - Nationell strategi för cybersäkerhet 2025-2029. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/reports/SE_NCSS_2025_se.pdf

Government of Sweden (2024) NCSS – Official document, Nationell strategi för cybersäkerhet 2025-2029. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/SE_NCSS_2025_OFFICIAL_DOCUMENT_se.pdf

Government of Sweden (2025) NCSS Annex 2, Bilaga 2: Organisationer med roller och ansvarsområden inom cybersäkerhet Nationell strategi för cybersäkerhet 2025–2029. Available at: https://www.enisa.europa.eu/sites/default/files/ncss-map/strategies/additional-documents/SE_NCSS_2025_ANNEX_2_se.pdf

Government of Sweden (2025) NCSS Annex 1, Bilaga 1: Handlingsplan, Nationell strategi för cybersäkerhet 2025-2029. Available at: https://www.regeringen.se/contentassets/0903061f79204084b6acf4ce1a978830/bilaga-1-handlingsplan.pdf

Government of Sweden (2023) Revision report, Riksrevisionens rapport om regeringens styrning av samhällets informations- och cybersäkerhet. Available at: https://www.regeringen.se/contentassets/cd23ea9b36fd4d59b990f7541023214d/riksrevisionens-rapport-om-regeringens-styrning-av-samhallets-informations--och-cybersakerhet-skr.-20232426.pdf

A.3 Maturity models and indices

Cybersecurity Maturity Model Certification (CMMC), CMMC Assessment Guide (Level 2), Available from: https://www.acq.osd.mil/cmmc/docs/CMMC-Assessment-Guide-Level-2-v2.0.pdf

Harvard Kennedy School - Belfer Center (2025) Cybersecurity Strategy Scorecard. Available at: https://www.belfercenter.org/research-analysis/cybersecurity-strategy-scorecard

Harvard Kennedy School – Belfer Center (2025) Cybersecurity Strategy Scorecard. Available at: https://www.belfercenter.org/sites/default/files/2025-03/Cyber%20Strategy%20Scorecard_3.1.pdf

Institute of Internal Auditors (2017) Internal Audit Capability Model (IA-CM) for the Public Sector: IA-CM Assessment Tool. Available at: https://iia-dl.theiia.org/BookstorePublic/IA-CM%20Assessment%20Tool.docx

International Telecommunication Union (2024) Global Cybersecurity Index 2024 5th edition (GCI). Available at: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

International Telecommunication Union (2025) Global Cybersecurity Index. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx

MIT Technology Review (2022) MIT Cyber Defence Index (CDI) 2022/2023. Available at: https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defence-index-2022-23/

MIT Technology Review Insights (2022) MIT Cyber Defence Index (CDI) 2022/2023, Methodology White Paper, Available at: https://mittrinsights.s3.amazonaws.com/CDIreport.pdf

Public Expenditure and Financial Accountability (2023) (Internal Audit Capability Model (IA-CM) - Institute of Internal Auditors. Available from: https://www.pefa.org/sites/pefa/files/PEFA%202022%20Stocktaking%20-%20B25.pdf

University of Oxford – Oxford-Martin School (2021) Development and Evolution of the CMM. Available at: https://gcscc.ox.ac.uk/development-and-evolution-of-the-cmm

University of Oxford – Global Cyber Security Capacity Centre (GCSCC) (2021), Cybersecurity Capacity Maturity Model for Nations (CMM). Available at: https://gcscc.web.ox.ac.uk/files/cmm2021editiondocpdf

U.S Department of Energy - Office of Cybersecurity, Energy Security, and Emergency Response (2022) Cybersecurity Capability Maturity Model (C2M2) Version 2.1 of June 2022, Available at: https://c2m2.doe.gov/Documents/C2M2-v2-1.pdf

U.S Department of Energy - Office of Cybersecurity, Energy Security, and Emergency Response (2022) Self-Evaluation Guide: Companion Document to C2M2 Version 2.1 of June 2022, Available at: https://c2m2.doe.gov/C2M2%20Self-Evaluation%20Guide.pdf

U.S. Department of Energy (2022) Cybersecurity Capability Maturity Model (C2M2), Available at: https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

U.S. Department of Defence – Chief Information Officer (2025) Cybersecurity Maturity Model Certification (CMMC). Available at: https://dodcio.defence.gov/CMMC/

U.S. Department of Defence (2024) Federal Register / Vol. 89 / Rules and Regulations of 15 October 2024, Cybersecurity Maturity Model Certification (CMMC) Program. Available at: https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

SECTION 5

Annex B – Maturity models review

Annex B – Maturity models review

Research on the methodology of maturity models continues to evolve and since the publication of the original NCAF in 2020, a range of recognised maturity models and indices has been published including:

- Cybersecurity Capacity Maturity Model for Nations (CMM),
- Cybersecurity Capability Maturity Model (C2M2),
- Cybersecurity Maturity Model Certification (CMMC),
- Internal Audit Capability Model (IA-CM),
- Cybersecurity Strategy Scorecard,
- Global Cybersecurity Index (GCI); and
- Cyber Defence Index (CDI).

A detailed review of these models highlighted both enduring principles and significant developments since 2020. The following subsections analyse the changes in each model across four key elements: **attributes/dimensions, maturity levels, assessment methods and results representation**.

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

The Cybersecurity Capacity Maturity Model for Nations (CMM), developed in 2014 by the Global Security Capacity Centre (GCSCC) at the University of Oxford, is a framework designed to help nations assess and strengthen their overall cybersecurity capacity. It provides a structured approach to evaluate a country's readiness, identify gaps, and guide the development of effective policies, skills, and practices aimed at building national cyber resilience. After initial pilot deployment, the model was revised in 2017 to refine its structure and factors. The 2021 edition incorporated lessons learned from the worldwide implementation and addressed emerging challenges, with a stronger focus on digital inclusion, data protection, and resilience to disinformation, areas that were less emphasized in the earlier version.

Attributes/Dimensions

The CMM defines five core dimensions that collectively represent the full spectrum of national cybersecurity capacity:

- **Cybersecurity Policy and Strategy**: Focuses on the development and implementation of national cybersecurity strategies, incident response, critical infrastructure protection, and defence integration.
- **Cybersecurity Culture and Society**: Assesses societal awareness, trust in online services, user understanding of privacy, reporting mechanisms, and the role of media in shaping cybersecurity attitudes.
- **Building Cybersecurity Knowledge and Capabilities**: Evaluates awareness programs, formal education, professional training, and research and innovation efforts.
- **Legal and Regulatory Frameworks:** Reviews the existence and effectiveness of laws and regulations related to cybersecurity, cybercrime, data protection, and judicial capacity.
- **Standards and Technologies**: Examines the adoption of cybersecurity standards, deployment of security controls, software quality, infrastructure resilience, and responsible disclosure practices

Each dimension is broken down into Factors, which are further divided into Aspects, and measured using Indicators that reflect specific actions or capabilities.

Maturity levels

- The CMM uses a five-stage maturity scale to assess progress within each aspect:
- **Start-up:** No or minimal capacity; early discussions may exist but lack formalisation.
- **Formative:** Initial structures or policies are emerging; activities may be ad hoc or fragmented.
- **Established:** Systems and processes are in place and functioning; evidence of effectiveness exists.
- **Strategic:** Capacity is aligned with national priorities; decisions are informed by risk assessments and strategic planning.
- **Dynamic:** Capacity is adaptive, forward-looking, and contributes to global leadership; mechanisms exist to respond to evolving threats and technologies

Each stage includes a set of binary indicators that must be evidenced to confirm attainment.

Assessment method

The CMM assessment is conducted through a combination of:

- In-country stakeholder consultations
- Desk research and document analysis
- Evidence-based scoring against indicators

The process is collaborative and multi-stakeholder, involving government, private sector, academia, and civil society. The output is a detailed report that benchmarks national capacity, identifies gaps, and recommends targeted actions for improvement

Results representation

Results are presented in a structured format. Each country is scored across all five dimensions and their respective factors. Maturity levels are assigned per aspect, based on fulfilment of indicators. The final report includes:

- Visual maturity map
- Narrative analysis of strengths and weaknesses
- Prioritised recommendations for capacity building
- Guidance for strategic investment and policy development

This format enables countries to track progress over time, compare with peers, and align cybersecurity efforts with broader national goals.

B.2 Cybersecurity Capability Maturity Model (C2M2)

The Cybersecurity Capability Maturity Model (C2M2) was developed by the U.S. Department of Energy (DOE) to assist organisations in evaluating and enhancing their cybersecurity capabilities. Initially released in 2014 (version 1.1), C2M2 aimed to provide a structured approach for assessing cybersecurity maturity and guiding improvements. The model underwent significant updates in July 2021, consolidating previous sector-specific versions (electricity, oil and natural gas sectors) into a unified framework tailored for the energy sector. The most recent update, version 2.1, was released in

June 2022. This version refined the model based on real-world testing and user feedback, enhancing its applicability and effectiveness in addressing evolving cybersecurity challenges in the energy sector. C2M2 serves as a valuable tool for organisations seeking to strengthen their cybersecurity posture and resilience against emerging threats.

Attributes/Dimensions

The C2M2 model continues to be built around the same ten core domains, each representing a distinct cybersecurity capability area with associated management and approach objectives. With version 2.1, the overall framework and domain structure remained unchanged, but two-thirds of the practices were revised.

Maturity levels

The C2M2 model uses a scale of maturity indicator levels:

- MIL0 – no practice performed
- MIL1 – Initiated
- MIL2 – Performed
- MIL3 – Managed

The content and the description of the MILs stayed the same as per the previous version.

Assessment method

While still designed for self-assessment, newer toolkits (C2M2 Toolkit) and resources have been developed to enable more structured scoring, prioritisation of domains, and longitudinal tracking. Assessments can be conducted as facilitated workshops or self-evaluation, allowing flexibility depending on organisational needs.

Results representation

The C2M2 Self-Evaluation Report provides a structured visual summary of the assessment results, generated once all responses are entered into the self-evaluation tool. The core visualisation is a 3x10 matrix of donut charts, where each chart represents one domain at a specific Maturity Indicator Level (MIL). The coloured segments indicate the number of practices rated as: “Fully Implemented (FI)”, “Largely Implemented (LI)” - dark and light blue, or as “Partially Implemented (PI)”, “Not implemented (NI)” - light and dark yellow. In addition, the report features horizontal bar charts showing implementation levels for each practice within a domain, as well as domain-specific summaries that break down results by objectives. A separate Management Practices summary highlights how institutionalised cybersecurity activities are across all domains.

B.3 Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification (CMMC), initially designed for U.S. Department of Defence contractors to strengthen cybersecurity across the Defence Industrial Base and protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). Although focused on the U.S. context, its modularity makes it a valuable reference for supply chain resilience and auditability. CMMC 1.0 was introduced in 2020, and since then it has undergone several changes. In CMMC 2.0 (announced in 2021), implementation guidance has been fully aligned with NIST 800-171 and SP 800-172 and introduced more flexibility (e.g., Plans of Action and Milestones – POA&M). The

final rule of CMMC 2.0 was published in October 2024, with phased implementation expected through 2025, including the activation of CMMC Level 2 self-assessments effective on February 2025.

Attributes/Dimensions

The CMMC 1.0 included 17 capability domains, each containing multiple practices and processes to be evaluated. It focused on assessing both presence and institutionalisation of cybersecurity practices at different maturity levels. This approach led to a relatively large number of assessment items, contributing to complexity in implementation and auditing. In contrast CMMC 2.0 simplifies this structure significantly by reducing the number of domains and focusing directly on the implementation of specific security controls derived from earlier mentioned NIST standards. The explicit concept of multiple dimensions was removed, favouring a more streamlined approach. This results in fewer total assessment requirements, making the certification process more straightforward and practical for organisations.

Maturity levels

The Cybersecurity Maturity Model Certification (CMMC) defines three levels of cybersecurity maturity, each reflecting a different degree of protection for sensitive government information.

- **Level 1:** focuses on basic safeguarding of Federal Contract Information (FCI). Organisations at this level are expected to meet a set of 15 requirements from FAR clause 52.204–21 and confirm compliance through an annual self-assessment.
- **Level 2:** is designed to protect Controlled Unclassified Information (CUI). It includes a broader set of requirements based on NIST standards (110 security requirements from NIST SP 800–171 R2). Depending on the sensitivity of the contract, organisations may either self-assess or undergo a formal third-party certification. In some cases, partial compliance is allowed temporarily, provided there's a clear plan to close the gaps within a set timeframe.
- **Level 3**: applies to the most sensitive environments, where protection against Advanced Persistent Threats (APTs) is essential. It builds on Level 2 and additionally adds 24 enhanced requirements from NIST SP 800–172. Certification at this level is conducted by a government-led assessment team and must be renewed every three years.

Each level is tied to the type of information handled and the level of assurance the Department of Defence requires from its contractors.

Assessment method

CMMC assessments are conducted to verify that an organisation has implemented the required cybersecurity controls. The method depends on the level:

- **Level 1:** Organisations perform a self-assessment annually to confirm that basic security practices are in place. This can be done internally or with help from a third party, but it remains a self-assessment.
- **Level 2:** Depending on the contract, organisations either self-assess or hire a certified third-party assessor (C3PAO). Certification assessments are required every three years and must cover all systems that handle Controlled Unclassified Information (CUI).
- **Level 3:** This level requires a government-led assessment by DCMA DIBCAC. Before starting, the organisation must already hold a valid Level 2 certification. The Level 3 assessment is more rigorous and occurs every three years.

Each assessment follows a defined scope, based on which systems process, store, or transmit sensitive data. If some requirements are not met, the organisation may receive a conditional status and must resolve the gaps within 180 days.

Results representation

Assessment results are recorded and submitted to the Department of Defence using secure systems (SPRS or eMASS). The outcome is documented in a formal Assessment Findings Report, which includes:

- A score based on how many requirements were met.
- A breakdown of findings: each requirement is marked as Met, Not Met, or Not Applicable.
- If applicable, a Plan of Action and Milestones (POA&M) listing items to be fixed.

Organisations must also submit an affirmation—a statement confirming they continue to meet the requirements. This is done annually, even if the certification is valid for three years. If an organisation disagrees with the assessment outcome, it can initiate a formal appeal process.

B.4 Internal Audit Capacity Model (IA-CM) for the Public Sector

The Internal Audit Capability Model (IA-CM) is a structured framework designed to assess and develop the maturity of internal audit functions within the public sector. It was originally developed between 2006 and 2009 under the auspices of the Institute of Internal Auditors Research Foundation (IIARF), in response to the need for a universal tool that could evaluate internal audit capabilities across diverse jurisdictions and organisational structures. IA-CM enables organisations to identify their internal audit requirements, assess current capabilities, and define a roadmap for improvement.

In 2022, the model was significantly expanded through its integration into the broader Public Expenditure and Financial Accountability (PEFA) framework, where it serves as a diagnostic tool for analysing the internal audit performance indicator PI-26. This formal linkage elevated IA-CM's role in public financial management and positioned it as a reference standard for evaluating audit effectiveness and institutional alignment.

Further enhancements followed in 2023, when IA-CM was supplemented with digital self-assessment tools and structured templates. These additions support more efficient implementation by internal audit teams, senior management, and legislators.

Today, IA-CM functions not only as a methodological framework but also as a strategic instrument for quality assurance, capacity planning, and reinforcing the credibility of internal audit as a cornerstone of public sector governance.

Attributes/Dimensions

The IA-CM Assessment Tool is structured around six core dimensions, referred to as "internal audit elements of the IA-CM." These are:

- Services and Role of Internal Auditing
- People Management
- Professional Practices
- Performance Management and Accountability
- Organisational Relationships and Culture

- Governance Structures

Each element is further broken down into Key Process Areas (KPAs), which represent clusters of related activities that, when institutionalised, contribute to achieving a specific capability level.

Maturity levels

- IA-CM defines five progressive capability levels that reflect the maturity of an internal audit function:
- **Level 1** – Initial: No sustainable, repeatable capabilities; dependent on individual effort.
- **Level 2** – Infrastructure: Sustainable and repeatable internal audit practices and procedures.
- **Level 3** – Integrated: Internal audit management and professional practices are uniformly applied.
- **Level 4** – Managed: Internal audit integrates information across the organisation to improve governance and risk management.
- **Level 5** – Optimising: Internal audit learns from internal and external sources to drive continuous improvement.

Each level is achieved only when all KPAs at that level are mastered and institutionalised

Assessment method

The IA-CM assessment is typically conducted as a self-assessment, though it may be externally validated or independently performed. The process includes:

- Understanding the IA-CM model
- Identifying institutionalised KPAs
- Reviewing documentation on the internal audit activity and its environment
- Interviewing senior managers and stakeholders
- Confirming capability level based on institutionalised KPAs
- Communicating results

Results representation

The IA-CM model is visually represented as a one-page matrix:

- **Vertical axis:** Capability levels (1 to 5), increasing from bottom to top
- **Horizontal axis:** Elements of internal auditing
- **Cells:** KPAs for each level and element

This matrix illustrates the extent to which the internal audit activity influences each element at a given maturity level.

The final assessment result includes:

- A profile of strengths and areas for improvement
- The overall capability level, defined as the lowest level for which all KPAs are institutionalised
- A summary report with conclusions, recommendations, and comparison to organisational needs
- Identification of leading practices and a roadmap for improvement.

B.5 The Cybersecurity Strategy Scorecard

Cybersecurity Strategy Scorecard 3.1 is a strategic evaluation framework developed in 2025 by specialists from the Harvard Kennedy School, specifically under the Belfer Centre for Science and International Affairs. The Scorecard provides a comparative analysis of national cybersecurity strategies from seven major cyber powers—Australia, Germany, Japan, Singapore, South Korea, the United Kingdom, and the United States. Building on previous Belfer Centre research such as the 2022 National Cyber Power Index, this edition aims to identify best practices, highlight policy gaps, and offer actionable recommendations for future strategy development. It combines qualitative and quantitative data, expert interviews, and document analysis to guide policymakers in designing forward-looking, context-sensitive cybersecurity strategies.

Attributes/Dimensions

The Scorecard evaluates national cybersecurity strategies across five core categories, each broken down into sub-categories and detailed elements:

- **Protecting People and Infrastructure**: Assesses how strategies address national cyber defence, including critical infrastructure, personal data, supply chains, SMEs, and vulnerable populations.
- **Generating Capacity**: Evaluates how countries build the human and institutional capabilities needed for cybersecurity, including workforce development and education.
- **Building Partnerships**: Measures collaboration with domestic and international stakeholders, including public-private partnerships and interagency coordination.
- **Codifying Roles and Responsibilities**: Examines how clearly countries assign duties to cyber-relevant agencies and establish procedural and technical requirements such as incident reporting.
- **Communicating Clear Policy**: Assesses how well the strategy articulates its vision, sets accountability mechanisms, and communicates implementation plans.

These categories are further divided into 18 sub-categories and 70 subject elements, supported by 268 binary criteria used internally to reduce subjectivity in scoring.

Assessment method

The Scorecard uses a relative scoring approach rather than absolute numerical scores. Each country is evaluated against the other six and classified as:

- Leading
- Meeting the Bar
- Lagging

This method avoids arbitrary weightings and allows for more nuanced comparisons. The evaluation is based on:

- Publicly available strategy documents
- Supporting materials directly related to national strategies
- Expert interviews with policymakers, researchers, and practitioners from each country

It's important to note that, the methodology emphasises intent over implementation, focusing on the strategic vision rather than real-world outcomes. This is due to the inherent difficulty in measuring cybersecurity effectiveness and the lack of publicly available data on implementation. The approach is

designed to highlight policy innovation and strategic clarity, making it a valuable tool for benchmarking and future strategy development

B.6 The Global Cybersecurity Index (GCI)

The Global Cybersecurity Index (GCI) assesses the cybersecurity capabilities of countries worldwide, focusing on governmental frameworks and policies. Launched by the International Telecommunication Union (ITU) in 2015, the GCI aims to highlight best practices and encourage improvements across various sectors. The 2024 update enhances its relevance by providing more detailed insights into country-specific strategies and challenges. Ultimately, the GCI promotes a more secure global cyberspace through improved national preparedness, leveraging the expertise of diverse organisations to foster international cooperation and facilitate knowledge exchange.

Attributes/Dimensions

The GCI focuses on five key pillars: Legislative Measures, Technical Measures, Organisational Measures, Capacity Development Measures, and Cooperation Measures.

- Legislative Measures
- Technical Measures
- Organisational Measures
- Capacity Development Measures
- Cooperation Measures
- Assessment method

The GCI employs a mixed-method approach, utilising both quantitative and qualitative data to evaluate national cybersecurity capabilities. Countries complete a structured questionnaire that collects information across the defined pillars, which is then analysed to generate overall scores. The methodology emphasises a self-assessment process, allowing countries to report on their cybersecurity measures and initiatives.

B.7 The Cyber Defence Index (CDI)

The Cyber Defence Index (CDI) is a national-level benchmark developed by MIT Technology Review Insights, first published in 2022/2023. It evaluates how well major economies, primarily the G20, have adopted technological and policy measures to resist cyberattacks and enable secure digital operations.

Attributes/Dimensions

This index evaluates 20 leading digital economies across governance, resilience, capability, and trust. It applies several measured indicators grouped into four weighted pillars:

- Critical Infrastructure
- Cybersecurity Resources
- Organisational Capacity and
- Policy Commitment.
- Assessment method

The Cyber Defence Index uses a multi-layered assessment approach, combining public data analysis, structured surveys of senior cybersecurity professionals and consultations with expert panellists.

These inputs are synthesised into 16 indicators across the four pillars, normalised and peer-reviewed to provide a comparative ranking.

TP-01-26-006-EN-N

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity
Athens OfficeAgamemnonos 14
Chalandri 15231, Attiki, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

Publications Office
of the European Union