EUROPEAN UNION AGENCY
FOR CYBERSECURITY

EU CYBERSECURITY INDEX

Framework and methodological note

MARCH 2024

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 eucsi-feedback@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

ENISA

LEGAL NOTICE

COPYRIGHT NOTICE

TABLE OF CONTENTS

1. EU CYBERSECURITY INDEX

1.1 OVERVIEW

Cybersecurity Act (Article 1(1), Article 3(1), Article 4(5), Recitals 6 and 15), notes that ENISA mandate and objectives are towards achieving a "high common level of cybersecurity across the Union" and support the EU and MS to "increase their cybersecurity capabilities". For ENISA to reach these objectives, an understanding of the current state of cybersecurity maturity across MS is necessary. Such an understanding would allow regular monitoring the level of cybersecurity across the EU and MS over the years and to reinforce their respective cybersecurity capabilities and leverage the robustness of the overall EU cybersecurity ecosystem.

The EU CSI (EU Cybersecurity Index) is a tool to describe the cybersecurity posture of MS (Member States) and the EU, which:

- Gives insights on the cybersecurity maturity and capabilities on individual countries and the EU.
- Helps identifying opportunities for peer-learning and improvement.
- Making the most of available data, information and knowledge on cybersecurity across the EU.
- Enables to evaluate their progress towards higher levels of cybersecurity vis-à-vis index indicators.

It is a composite index, with a hierarchical structure, as depicted in the following figure.

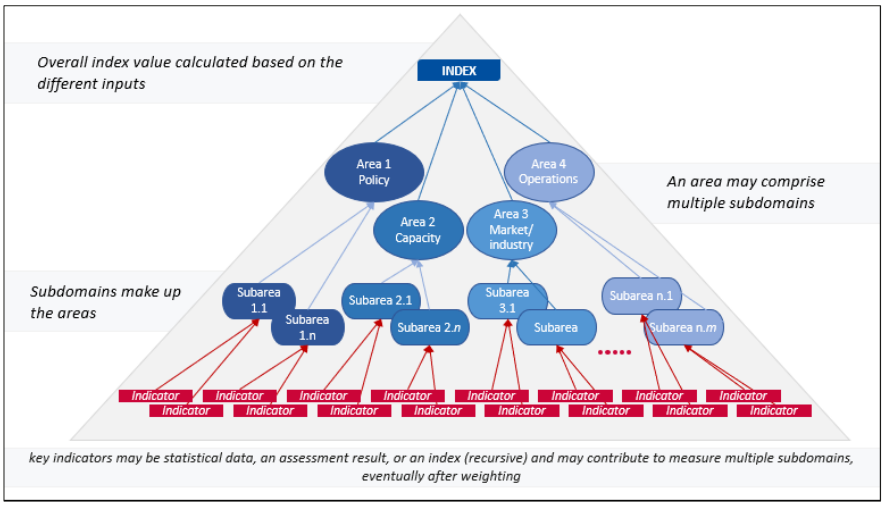

Figure 1. Design of the EU Cybersecurity Index

The index is comprised by 84 qualitative and quantitative indicators structured into 4 areas (policy, operations, capacity and market/industry) and 16 sub-areas/sub-domains. In addition, each sub-area is assigned a weight. Out of the 84 indicators, 60 are collected at MS level and aggregated at EU level, while 24 are EU-wide indicators. Key indicators may be statistical data, an assessment result, or an index (recursive) and may contribute to measure multiple subareas eventually after weighting.

The framework is applied to each EU Member State by calculating aggregated values (from 0 to 100) corresponding to a MS's cybersecurity posture for each area, sub-area, as well as an

overall value. More specifically, each subarea value is a weighted arithmetic mean of all indicators affecting it. Each area value is also a weighted arithmetic mean of all subareas affecting it. The overall index is an arithmetic mean sum of all areas.

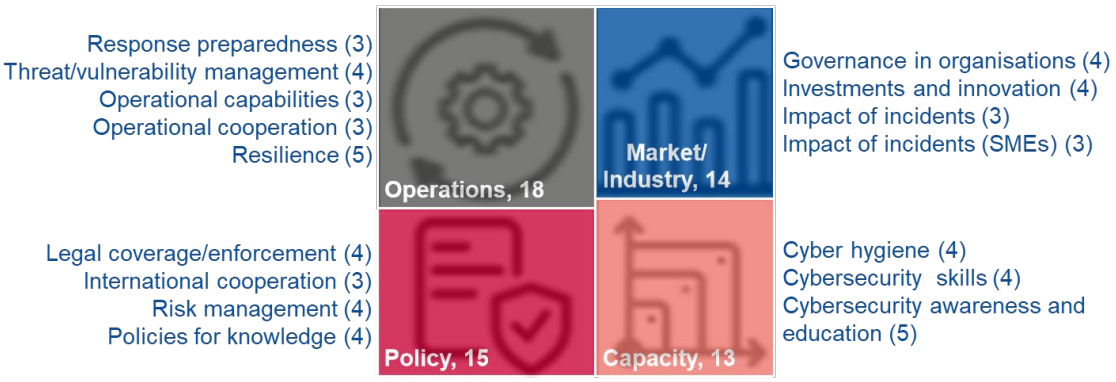

Figure 2. Areas, subareas and number of indicators

1.2 SCOPE

This document serves as the methodological note describing the purpose, structure and properties of the EU CSI and aims to provide a relevant overview for public consultation and feedback. The EU CSI was developed according to the guidelines and recommendations in the OECD/JRC's 'Handbook on constructing composite indicators: methodology and user guide'[1]. The data included in the EU CSI were mostly collected from the relevant authorities of the Member States by ENISA and from ad hoc studies launched by the ENISA and European Commission.

[1] Nardo M, Saisana M, Saltelli A, Tarantola S, Hoffmann A, Giovannini E. Handbook on Constructing Composite Indicators: Methodology and User Guide. Paris (France): OECD publishing; 2008. JRC47008
http://www.oecd.org/els/soc/handbookonconstructingcompositeindicatorsmethodologyanduserguide.htm

2. EU CSI STRUCTURE

2.1 DATA SOURCES

Most of the data in the EU CSI have been collected directly by national authorities via the ENISA National Liaison Officers (NLO) Network. Additional sources of data have been utilised as per the table below.

Data source	Data collection process
Eurostat	Data collected and verified by the national statistical offices or by Eurostat. https://ec.europa.eu/eurostat/data/database
Eurobarometer	Data collected by Eurobarometer, the polling instrument used by the European Commission, the European Parliament and other EU institutions and agencies to monitor regularly the state of public opinion in Europe on issues related to the European Union as well as attitudes on subjects of political or social nature. https://europa.eu/eurobarometer/screen/home
Council of Europe	Data collected by the Council of Europe in regards to Treaty No. 185 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
ISO (International Organisation for Standardization)	Data collected and verified by ISO via the Survey of Management System Certifications. The providers of the data are the certification bodies accredited by the IAF (International Accreditation Forum) MLA (Multilateral Recognition Arrangement) members. https://isotc.iso.org/livelink/livelink?func=ll&objId=21897526&objAction=browse&viewType=1
ENISA	Studies conducted by ENISA concerning data collection of MS and EU cybersecurity capacities https://www.enisa.europa.eu/
Shodan	Data collected via dedicated queries on the Shodan search engine. https://www.shodan.io/
European Commission – Horizon Dashboard	Data collected by European Commission Directorate-General for Research and Innovation via the Horizon Dashboard. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard

2.2 INDICATORS PER AREA/SUBAREA

There are 4 areas in the EU CSI (policy, operations, capacity, industry/market) and 16 subareas, comprising in total 60 indicators. In addition, 24 EU wide indicators measuring sectorial critical and maturity are considered for the calculation of the EU CSI. The table below lists the areas, subareas and number of indicators, thus showcasing the structure of the EU CSI.

Capacity	**13**
Cyber hygiene	**4**
Citizens: privacy and protection of personal data	1
Citizens: secure internet use	1
Large enterprises: ICT security measures	1
SMEs: ICT security measures	1
Cybersecurity awareness	**4**
Citizens: Knowledge of cybersecurity matters	1
Large enterprises: Staff Awareness	1
SMEs: Cybersecurity training	1
SMEs: Staff Awareness	1
Cybersecurity skills and education	**5**
Cybersecurity graduates in higher education	1
Cybersecurity exercises at national and international level	1
EU R&D funding	1
National level cybersecurity trainings	1
Tools and training to fight cybercrime	1
Market/Industry	**14**
Cybersecurity governance within organisations	**4**
Enterprises: ICT security policy	1
Enterprises: risk assessment	1
Organisations certified with relevant ISO standards	1
Supply chain management by essential/ important entities	1
Cybersecurity investments and innovation	**4**
Cybersecurity investments by essential/important entities	1
Enterprises buying security software applications as a cloud computing service	1
Enterprises using AI technologies for ICT security	1
SMEs: EU R&D funding	1
Large enterprises: Impact of cybersecurity incidents	**3**
Large enterprises: Security Incidents - Destruction or corruption of data	1
Large enterprises: Security Incidents - Disclosure of confidential data	1
Large enterprises: Security Incidents - Unavailability of ICT Services	1
SMEs: Impact of cybersecurity incidents	**3**
SMEs: Security Incidents - Destruction or corruption of data	1
SMEs: Security Incidents - Disclosure of confidential data	1
SMEs: Security Incidents - Unavailability of ICT Services	1
Operations	**18**
National-level response preparedness	**4**
CSIRT(s) certification	1

Dedicated cybercrime establishment within law enforcement and prosecution offices	1
Incident reporting implementation	1
Threat monitoring at national level	1
Operational cooperation	**4**
Cooperation at a national level	1
CSIRTs international presence	1
Establishment of a national reporting scheme for major cyber incidents	1
Establishment of operational cooperation mechanisms against cybercrime	1
Resilience of key operators	**6**
E-communications resilience (EECC) - cases	1
E-communications resilience (EECC) – duration	1
E-trust services resilience (e-IDAS) - cases	1
E-trust services resilience (e-IDAS) - duration	1
Participation by essential and important entities in a national or EU-level ISAC	1
Resilience of important/essential entities - cases	1
Threat and vulnerability management	**4**
Cyber-attack surface nationwide	1
Share of compromised IPs, services and servers	1
Use of secure internet standards	1
Vulnerability patching effectiveness	1
Policy	**15**
Coverage and enforcement of legal and regulatory framework	**4**
Coverage and implementation of objectives in national cybersecurity strategy	1
Coverage of essential sectors by national legislation	1
Coverage of vulnerability disclosure policies	1
Implementation of cybersecurity EU legislation	1
International cooperation	**3**
Alignment with the Council of Europe Convention on Cybercrime	1
Establishment of international cooperation mechanisms	1
International cooperation on cybersecurity	1
National-level risk management	**4**
Baseline cyber security risk management measures for essential/important entities	1
Definition and compliance of cybersecurity baseline(s) for essential and important entities	1
Identification of essential and important entities	1
Implementation of supervisory measures for essential and important entities	1
Policies for knowledge	**4**
Cybersecurity in higher education	1
Cybersecurity in national education curricula	1
Cybersecurity in R&D priorities and initiatives	1
National and international cooperation for cybersecurity R&D	1

2.3 LIST OF INDICATORS

Indicator	Algorithm	Source
Citizens: privacy and protection of personal data	% of individuals that managed access to personal data on the internet by performing at least one of the following actions: • read privacy policy statements before providing personal data • restricted or refused access to the geographical location • limited access to profile or content on social networking sites or shared online storage • refused allowing the use of personal data for advertising purposes • checked that the website where personal data provided was secure	Eurostat
Citizens: secure internet use	% of Internet users who changed the way they use the internet due to security concerns	Eurobarometer
Large enterprises: ICT security measures	% of large enterprises using at least one of the following ICT security measures: • Strong password authentication • Combination of at least two authentication mechanisms (e.g. user-defined password, one-time password (OTP), code generated via a security token or received via a smartphone, biometric methods) • Encryption techniques for data, documents or e-mails • Data backup to a separate location (including backup to the cloud) • Network access control (management of access by devices and users to the enterprise's network) • VPN (Virtual Private Network extends a private network across a public network to enable secure exchange of data over public network) • Maintenance of log files for analysis after security incidents • Performance of ICT security tests	Eurostat
SMEs: ICT security measures	Weighted average of: • Share of enterprises using strongpassword authentication • Share of enterprises using encryption techniques for data, documents or e-mails • Share of enterprises using data backup to a separate location (including backup to the cloud) • Share of enterprises using VPN (Virtual Private Network extends a private network across a	Eurostat

	public network to enable secure exchange of data over public network) • Share of enterprises maintaining log files for analysis after security incidents • Share of enterprises performing ICT security tests	
Citizens: Knowledge of cybersecurity matters	% of internet users who feel very-well/well informed about the risks of cybercrime and/or are aware of the existence of a website, email address, online form, or contact number in their country where they can report a cybercrime or any other illegal online behaviour (e.g. cyberattack, online harassment or bullying)	Eurobarometer
Large enterprises: Staff Awareness	% of large enterprises that make persons employed aware of their obligations in ICT security related issues	Eurostat
SMEs: Cybersecurity training	% of SMEs: • that provided their employees with training or awareness raising about the risks of cybercrime in the last 12 months and/or • whose management feels that they are very well/well informed about the risks of cybercrime and/or • whose employees feel that they are very well/well informed about the risks of cybercrime	Eurobarometer
SMEs: Staff Awareness	% of SMEs that make persons employed aware of their obligations in ICT security related issues	Eurostat
Cybersecurity graduates in higher education	Normalised count of cybersecurity graduates enrolled in higher education curricula	ENISA
Cybersecurity exercises at national and international level	Scoring based on adapted NCAF[2] maturity levels, objective 6 "Organise cybersecurity exercises"	MS Survey
EU R&D funding	Share of EU R&D funding awarded per country for cybersecurity topics	EC Horizon Dashboard
National level cybersecurity trainings	Scoring based on adapted NCAF maturity levels, objective 7 "Strenghten training and educational programmes"	MS Survey
Tools and training to fight cybercrime	Scoring based on adapted NCAF maturity levels, objective 12 "Address cybercrime"	MS Survey

[2] https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

Enterprises: ICT security policy	% of enterprises that have document(s) on measures, practices or procedures on ICT security	Eurostat
Enterprises: risk assessment	% of enterprises performing a cybersecurity risk assessment	Eurostat
Organisations certified with relevant ISO standards	% of organisations certified with at least one of the following standards: ISO 22301:2019 (Business continuity management systems); ISO 27001:2013 (Information security management systems); ISO 28000:2007/ISO 28000:2022 (Security management systems)	ISO
Supply chain management by essential/ important entities	Average % of surveyed essential/important entities with third -party risk management policies	ENISA
Cybersecurity investments by essential/important entities	Average % of information security budget spending by surveyed essential/important entities as part of their overall IT budget/spending	ENISA
Enterprises buying security software applications as a cloud computing service	% of enterprises that buy security software applications (as a cloud computing service)	Eurostat
Enterprises using AI technologies for ICT security	Share of enterprises using AI technologies for ICT security	Eurostat
SMEs: EU R&D funding	Share of EU R&D funding awarded to private SMEs for Horizon Europe calls related to cybersecurity	EC Horizon Dashboard
Large enterprises: Security Incidents - Destruction or corruption of data	% of Large enterprises that did not experience ICT security related incidents leading to: destruction or corruption of data (e.g. due to infection of malicious software or unauthorised intrusion, hardware or software failures)	Eurostat
Large enterprises: Security Incidents - Disclosure of confidential data	% of Large enterprises that did not experience ICT security related incidents leading to: disclosure of confidential data (e.g. due to intrusion, pharming, phishing attack, actions by own employees (intentionally or unintentionally)	Eurostat

Large enterprises: Security Incidents - Unavailability of ICT Services	% of Large enterprises that did not experience ICT security related incidents leading to: unavailability of ICT services (e.g. Denial of Service attacks, ransomware attacks, hardware or software failures)	Eurostat
SMEs: Security Incidents - Destruction or corruption of data	% of SMEs that did not experience ICT security related incidents leading to: destruction or corruption of data (e.g. due to infection of malicious software or unauthorised intrusion, hardware or software failures)	Eurostat
SMEs: Security Incidents - Disclosure of confidential data	% of SMEs that did not experience ICT security related incidents leading to: disclosure of confidential data (e.g. due to intrusion, pharming, phishing attack, actions by own employees (intentionally or unintentionally)	Eurostat
SMEs: Security Incidents - Unavailability of ICT Services	% of SMEs that did not experience ICT security related incidents leading to: unavailability of ICT services (e.g. Denial of Service attacks, ransomware attacks, hardware or software failures)	Eurostat
CSIRT(s) certification	% of FIRST certified CSIRTs	ENISA
Dedicated cybercrime establishment within law enforcement and prosecution offices	Scoring based on adapted NCAF maturity levels, objective 12 "Address cybercrime"	MS Survey
Incident reporting implementation	Scoring based on adapted NCAF maturity levels, objective 13 "Establish incident reporting mechanisms"	MS Survey
Threat monitoring at national level	Scoring based on adapted NCAF maturity levels, objective 11 "Protect critical information infrastructure"	MS Survey
Cooperation at a national level	Degree of cooperation between national cybersecurity authorities/entities/actors	MS Survey
CSIRTs international presence	% of CSIRTs that participate in international activities	ENISA

Establishment of a national reporting scheme for major cyber incidents	Scoring based on adapted NCAF maturity levels, objective 13 "Establish incident reporting mechanisms"	MS Survey
Establishment of operational cooperation mechanisms against cybercrime	Scoring based on adapted NCAF maturity levels, objective 12 "Address cybercrime"	MS Survey
E-communications resilience (EECC) - cases	Number of cases reported as per EECC Art. 40	ENISA
E-communications resilience (EECC) – duration	Duration of total cases reported as per EECC Art. 40	ENISA
E-trust services resilience (e-IDAS) - cases	Number of cases reported as per eIDAS Art. 19	ENISA
E-trust services resilience (e-IDAS) - duration	Duration of total cases reported as per eIDAS Art. 19	ENISA
Participation by essential and important entities in a national or EU-level ISAC	% of essential and important entities across sectors participating in national or EU level ISACs	MS Survey
Resilience of important/essential entities - cases	Normalised number of cases reported for NIS1/NIS2 important and essential entities	ENISA
Cyber-attack surface nationwide	Average of the following variables normalised by IPs: • Vulnerability - Number of IPs that are exposed to at least one vulnerability • SSL Expired - Number of IPs with expired SSL certificate • SSL Old Protocol - Number of IPs with old protocols • SSL self-signed - Number of IPs with self-signed SSL • OS Linux - Number of IPs with old OS Linux • OS Windows - Number of IPs with old OS Windows • Port - Number of IPs with Ports considered that should not be publicly • available on Internet (port 23,161,68,69,80,81,110,137,389,445,3389,5353)	Shodan

	• Banner - Number of IPs with "authentication disabled" banner	
Share of compromised IPs, services and servers	Average (normalised by number of IPs) of: • Title - Number of websites with title containing "hacked by" or "0wn3d by" • Banner - Number of IPs containing "hacked by" text in published banner • Tag - Number of Compromised IPs, command and control servers (C2) as marked by Shodan • Product - Number of IPs with known security offensive tools	Shodan
Use of secure internet standards	Average (normalised by number of IPs) of: • SSL - Number of IPs using only modern TLS protocols without potential vulnerabilities, self-signed or expired certificates • IPv6 - Number of IPs version6 without old SSL/TLS protocols, potential vulnerabilities, self-signed or expired certificates • Banner - Number of websites with banners publishing "Content Security Policy" without old SSL/TLS protocols, potential vulnerabilities, self-signed or expired certificates	Shodan
Vulnerability patching effectiveness	Average normalised number of IPs exposed to the Shodan top-10 and ENISA Threat Landscape top vulnerabilities.	Shodan
Coverage and implementation of objectives in national cybersecurity strategy	Level of coverage and degree of implementation of objectives in national cybersecurity strategy as per the provisions of NIS2 for national cybersecurity strategies	MS Survey
Coverage of essential sectors by national legislation	Weighted average of coverage of national legislation concerning NIS2 sectors or other sectors	MS Survey
Coverage of vulnerability disclosure policies	Weighted average of sectors covered by vulnerability disclosure policies and the status of national coordinated vulnerability disclosure policies	MS Survey
Implementation of cybersecurity EU legislation	State of eligible (cybersecurity related parts of) Directives/Regulations • 100% if the Directive is fully transposed (notification sent to the EC) and entered into force	MS Survey

	• 70% when legislation has been transposed (notification sent to the EC), but entry into effect is in the future. • 40% when national legislation partially covers Directive requirements, but full transposition is pending. • 0% otherwise	
Alignment with the Council of Europe Convention on Cybercrime	Alignment with the Convention on Cybercrime (ETS No. 185); the first protocol on xebophobia and racism (ETS No. 189) and the second additional protocol on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)	Council of Europe
Establishment of international cooperation mechanisms	Scoring based on adapted NCAF maturity levels, objective 17 "Engage in international cooperation (not only with EU MS)"	MS Survey
International cooperation on cybersecurity	Scoring based on adapted NCAF maturity levels, objective 17 "Engage in international cooperation (not only with EU MS)"	MS Survey
Baseline cyber security risk management measures for essential/important entities	Weighted average of different baseline cyber security risk management measures for essential/important entities	MS Survey
Definition and compliance of cybersecurity baseline(s) for essential and important entities	Weighted EU average of relevant mechanisms in place at national level	MS Survey
Identification of essential and important entities	% of updated registries for essential and important cybersecurity entities	MS Survey
Implementation of supervisory measures for essential and important entities	% share of essential and important entities subjected to supervisory measures	MS Survey
Cybersecurity in higher education	Scoring based on adapted NCAF maturity levels, objective 7 "Strenghten training and educational programmes"	MS Survey

Cybersecurity in national education curricula	Scoring based on adapted NCAF maturity levels, objective 7 "Strenghten training and educational programmes"	MS Survey
Cybersecurity in R&D priorities and initiatives	Scoring based on adapted NCAF maturity levels, objective 8 "Foster R&D"	MS Survey
National and international cooperation for cybersecurity R&D	Scoring based on adapted NCAF maturity levels, objective 8 "Foster R&D"	MS Survey

3. METHODOLOGY

The index design follows the design methodology for dealing with composite indicators which was developed by the Organisation for Economic Co-operation and Development (OECD) in cooperation with the EU Joint Research Centre's Competence Centre on Composite Indicators and Scoreboards. Their methodology on Composite Indicators ("COIN") is described in a 10-step pocket guide[3] and a handbook[4].

This methodological note follows the example of the DESI (Digital Economy and Society Index) methodological note[5] made publicly available.

3.1 INDICATOR PROPERTIES

Indicators in the EU CSI comply with the following requirements:

- Must be collected on a regular basis. In order to fulfil the monitoring function, the indicators used in the index must be collected ideally on a yearly basis (or at least with a pre-defined regularity).
- Must be relevant for a policy area of interest. All indicators in the index must be accepted as relevant metrics in their specific policy areas.
- Must not be redundant. The index should not contain redundant indicators, either statistically or in terms of interpretation.

Indicators in the EU CSI adhere to the following properties:

- Valid: accurate measure of a behaviour, practice or task that is the expected output or outcome.
- Reliable: consistently measurable over time in the same way [e.g., by different observers].
- Precise: operationally defined in clear terms.
- Measurable: quantifiable [quantitative, qualitative or mix] using available tools and methods
- Timely: provides a measurement at time intervals relevant and appropriate in terms of the index objective.
- Objective: outcome achievement oriented.
- Transparent: the data collection process shall be transparent.
- Statistically valid: indicators should be statistically valid.
- Cost effective: balance the cost of collecting information with its usefulness.
- Attributable: 'owners' should be able to influence the performance measured by the indicator.
- Responsive: an indicator should be responsive to a change in the observed environment.
- Neutral: an indicator description and explanation should be unbiased in respect to MS specificities when used in a multi-national index.
- Validated and unassailable.
- Intelligible and easily interpreted (sufficiently simple to be interpreted in practice and intuitive).

[3] EC JRC, Your 10-Step Pocket Guide to Composite Indicators & Scoreboards, (2019) 12.
https://knowledge4policy.ec.europa.eu/sites/default/files/10-step-pocket-guide-to-composite-indicators-and-scoreboards.pdf
[4] OECD, Handbook on Constructing Composite Indicators: Methodology and User Guide, Paris, 2008.
https://www.oecd.org/sdd/42495745.pdf
[5] DESI Methodological Note, https://ec.europa.eu/newsroom/dae/redirection/document/88557

- The highest value of an indicator should be approachable in a reasonable way.
- Indicators should be replicable: results should be the same when an indicator value is produced by different people using the same method. The unit of measure should be easy to interpret.
- Information to derive an Indicator should not be too difficult or too expensive to collect. Therefore, indicators should ideally be based on data that is readily available, or on data that can be collected with a reasonable amount of effort.
- Indicator data shall be verifiable through correlation with secondary data.

3.2 DATA UPDATES AND CORRECTIONS

Updates and corrections are part of the lifecycle and nature of statistical data. It is typical that the values for one indicator suffer small amendments and only stabilise completely months or even years after the indicator was originally computed. This is the case for a significant number of EU CSI indicators. At each publication, historical data will also be reviewed to accommodate such changes.

3.3 NORMALISATION OF INDICATORS' VALUES

In order to aggregate indicators expressed in different units into the subareas and areas of the EU CSI, they have to be normalised. In EU CSI, normalisation is done using the min-max method, transforming the indicator values into a scale between 0 and 100. All indicators are designed to have a positive direction (i.e. where higher is better).

Take for example indicator X whose minimum value is equal to 0 and its maximum value is equal to 15. If a country has a raw value of 2.71 in this indicator, its normalized value will be:

$$\frac{2.71 - 0}{15 - 0} = \frac{2.71}{15} = 0.1806$$

We also scale this value to the interval [0,100] by multiplying by 100, resulting in the final normalised value 18.06.

3.4 IMPUTATION OF MISSING OBSERVATIONS

Imputation is the process of estimating missing data points. This can be done in any number of ways and the "best" way depends on the problem. In the EU CSI we had the following cases of missing data imputation and values for those observations were estimated using different methodologies, such as:

- Unconditional mean imputation method (the missing value for a country was replaced by the mean of the rest of the countries). The rationale behind this choice is that indicators are considered uncorrelated.
- Regression Imputation method: regression was performed using the indicators of the same subarea (Business continuity) per country.
- Mean imputation was used only when there were not too few with data for a particular indicator.

During the 2022 test run, the percentage of imputed values in the EU CSI was 10.72%.

3.5 WEIGHTS

For the EU CSI the following weights were used:

- At the indicator level: selection of weight is done by MS based on a series of principles, such as its impact and significance.

- At the sub-area level: same weights for all indicators. The rationale for this choice is that indicators are uncorrelated and there is no way of deciding which is more important in a subarea.
- At the area level: The weights selected from the previous phase (i.e. preparatory work in 2021/2022/2023) are used.
- At the Index level: same weight for all 4 areas to ensure balanced representation.

3.6 METHOD OF AGGREGATION

Concerning the method of aggregation, the approach followed by DESI is undertaken, namely weighted arithmetic mean. In DESI, the aggregation of indicators into sub-dimensions, of sub-dimensions into dimensions, and of dimensions into the overall index was performed from the bottom up using simple weighted arithmetic averages following the structure of the index (Figure 1).

As an example, the top-level score for country X was calculated using the formula:

Index(X) = Policy(X) * 0.25 + Market/Industry(X) * 0.25 + Operations(X) * 0.25 + Capacity(X) * 0.25

where Policy(X) for example is the score obtained by country X in the Policy area.

ABOUT ENISA

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

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14
Chalandri 15231, Attiki, Greece

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu