EU CYBERSECURITY INDEX (EU CSI) 2023 PILOT: UPDATED FRAMEWORK

1. BACKGROUND AND SCOPE

Since 2021 ENISA has been working on the development of a EU Cybersecurity Index, describing the cybersecurity posture of the EU and Member States (MS). Last year ENISA run the first pilot (EU-CSI 2022 Pilot), which has been updated and run this year as well (EU-CSI 2023).

The purpose of this document is to describe the structure and indicators of the EU-CSI 2023 Pilot.

The document is structured as follows:

- **Section 2**: Overview of EU-CSI
- **Section 3**: Weighting methodology
- **Section 4**: EU-Wide indicators
- **Section 5**: Changes with respect to the framework presented at the beginning of the year

Annexes
Annex I - Discontinued indicators
Annex II – Detailed list of indicators
Annex III – Statistical model overview

2. OVERVIEW OF EU-CSI

To support the EU in making informed decisions on identified challenges and gaps in cybersecurity, insights on the cybersecurity maturity and posture of the Union and Member State's policies, capabilities and operations are required. The objective of the EU-CSI is to provide this insight by:

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

The EU-CSI is a Composite Index, and its structure is depicted in the following figure.

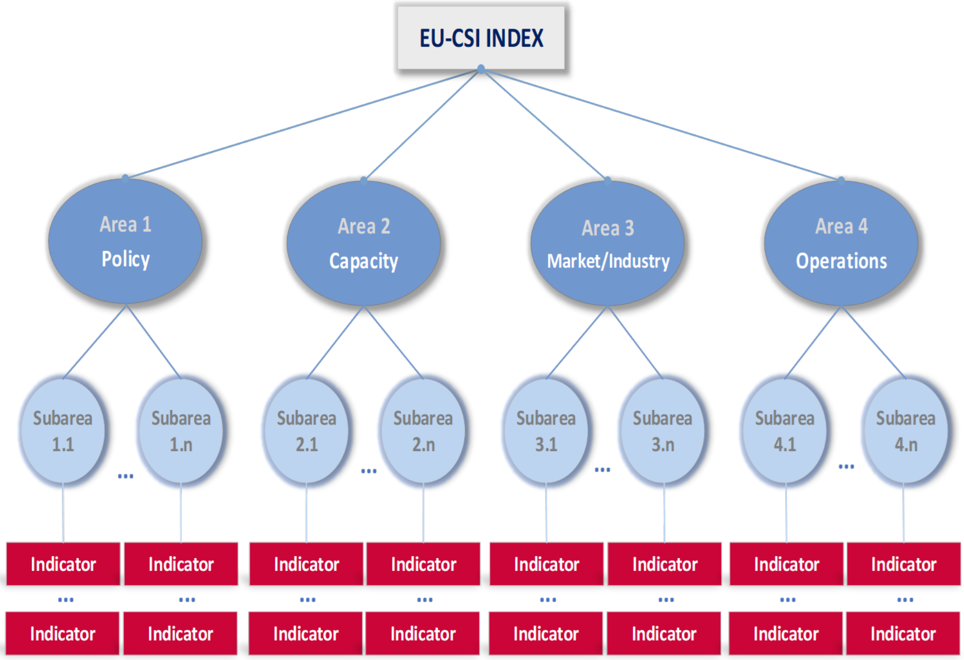

Figure 1: EU-CSI structure

The EU-CSI 2023 Pilot is composed by **60 indicators**, structured hierarchically across **16 sub-areas** and **4 areas.** The tables below show the indicators by area and sub-area. Each area and sub-area features a short description to facilitate the interpretation of the indicators. The tables below show the description of each area and sub-area, as well as the corresponding indicators.

Area: Capacity	**Ability of a MS to prevent, detect, and analyse cyber threats and incidents**
Sub-areas	
Cyber hygiene Implementation of measures for cyber-hygiene	• Enterprises: ICT security measures • Privacy and protection of personal data: citizens • Secure internet use by citizens • SMEs: ICT security measures
Cybersecurity awareness and education Societal knowledge of cybersecurity and efforts to increase cybersecurity awareness	• Cybersecurity (curricula) graduates in higher education • Enterprises: Staff Awareness • Knowledge of cybersecurity matters by citizens • SMEs: Awareness training • SMEs: Staff Awareness
Cybersecurity skills Availability of measures to increase specialised cybersecurity skills and knowledge	• Country share of EU R&D funding • Exercises at national and international level • National level cybersecurity trainings • Tools and training to fight cybercrime

Area: Market/Industry	**Ability of the private sector to prevent, detect, and analyse cyber threats and incidents.**
Sub-areas	
Cybersecurity governance within organisations Extent to which enterprises implement policy and measures to prevent cyber incidents	• Enterprises: ICT security policy • Number of organisations/enterprises certified with relevant ISO standards • Share of enterprises performing a risk assessment • Supply chain management by essential and important entities
Cybersecurity investments and innovation Extent to which enterprises invest into their current and future security	• Cybersecurity Investments by surveyed essential/important entities as part of their overall IT Budget/Spending • Share of enterprises that buy security software applications as Cloud Computing Service • Share of enterprises that use AI technologies for ICT security • Share of EU R&D funding to SMEs
Impact of cybersecurity incidents (SMEs) Extent to which SMEs have suffered from cybersecurity incidents	• Security Incidents: Destruction or corruption of data (SME) • Security Incidents: Disclosure of confidential data (SME) • Security Incidents: Unavailability of ICT Services (SME)
Impact of cybersecurity incidents Extent to which enterprises have suffered from cybersecurity incidents	• Security Incidents: Destruction or corruption of data (All Enterprises) • Security Incidents: Disclosure of confidential data (All Enterprises) • Security Incidents: Unavailability of ICT Services (All Enterprises)

Area: Operations	**Ability of a state to carry out operations to ensure resilience.**
Sub-areas	
National-level response preparedness Extent to which a country is prepared to deal with cyber-related issues	• Dedicated cybercrime establishment within law enforcement and prosecution offices • Incident reporting implementation • Threat monitoring at national level
National-level threat and vulnerability management National efforts for threat and vulnerability management	• Cyber-attack surface nationwide • Share of compromised IPs, services and servers • Use of secure internet standards • Vulnerability patching effectiveness
Operational capabilities Development of joint capabilities	• Certification of CSIRT(s) in a country • Participation by essential and important entities in a national or EU-level ISAC • Presence of a country's CSIRTs in the international cybersecurity arena
Operational cooperation Definition of a framework for cooperation at the national level	• Cooperation at a national level • Establishment of a national reporting scheme for major cyber incidents • Establishment of operational cooperation mechanisms against cybercrime
Resilience of key operators Resilience of key operators in terms of incidents and their duration	• E-communications resilience (EECC) - cases • E-communications resilience (EECC) – duration • E-trust services resilience (e-IDAS) - cases • E-trust services resilience (e-IDAS) - duration • Resilience of important/essential entities - cases

Area: Policy	**State of policy development and implementation**
Sub-areas	
Policies for knowledge and skills Definition of a policy framework for the development of knowledge and skills	• Cybersecurity in higher education • Cybersecurity in national education curricula • Cybersecurity in R&D priorities and initiatives • National and international cooperation for cybersecurity R&D
Coverage and enforcement of legal and regulatory framework Existence and coverage of national legislations	• Coverage and implementation of objectives in national cybersecurity strategy • Coverage of essential sectors by national legislation • Coverage of vulnerability disclosure policies • Implementation of cybersecurity EU legislation
International cooperation Alignment with international practices and policies	• Alignment with the CoE Convention on Cybercrime • Establishment of international cooperation mechanisms • International cooperation on cybersecurity
National-level risk management Coverage of risk-management at the national level	• Baseline cyber security risk management measures for essential/important entities • Definition and compliance of cybersecurity baseline(s) for essential and important entities • Identification of essential and important entities • Implementation of supervisory measures for essential and important entities

3. WEIGHTS

A weighting methodology has been devised to ensure that specific aspects of the indicators are reflected in the index calculation. Specifically, each indicator has been scored against a predetermined set of criteria and the sum of the normalised scores has been used as the indicator's weight. The weights per indicator can be found in the attached excel file.

The table below summarises the criteria and the possible scoring.

Criteria to define weights	Scoring
Impact of the indicator on an area Extent to which an indicator influences the relevant area.	**Score 0-1** • 1 = direct impact • 0.5 = indirect impact • 0 = no impact
Relevance for NIS2 implementation Extent to which an indicator conveys information about a country's NIS2 transposition and implementation	**Score 0-1** • 1 = direct relevance (refers to an obligation stated in the Directive) • 0.5 = indirect relevance (does not refer to an obligation stated in the Directive, but it contributes to it) • 0 = no relevance
Relevance indicated in the feedback survey Average of the scores indicated in the survey in the feedback.	**Score 0-5** • 5 = extremely relevant • 4 = quite relevant • 3 = somewhat relevant • 2 = limited relevance • 1 = no relevance

4. EU-WIDE INDICATORS

In addition to the indicators used to calculate the EU-CSI, a set of **24 "EU-wide indicators"** has been identified and it is used to give contextual information. These are indicators for which only data aggregated at the EU level is available and that are not used to calculate EU-CSI values.

These indicators are:

Indicator name
Implementation of cybersecurity measures by cloud service providers (CSPs) and cloud enablers
Implementation of cybersecurity measures by end users of cloud services
Impact of incidents on cloud service providers (CSPs) and cloud enablers

Indicator name
Impact of incidents on users of cloud services
Criticality of the following 10 sectors (one indicator per sector): Telecoms, Internet infrastructure, Trust services, Electricity, Gas, Oil, Finance, Health, Aviation, Rail
Maturity of the following 10 sectors (one indicator per sector): Telecoms, Internet infrastructure, Trust services, Electricity, Gas, Oil, Finance, Health, Aviation, Rail

5. CHANGES WITH RESPECT TO THE DRAFT 2023 EU-CSI

Earlier in 2023, a draft version of the EU-CSI framework has been presented. Based on ENISA's stakeholders' feedback 15 indicators have been deleted or frozen[1] on the following grounds:

- MS assessed their relevance with a low score in the survey used to ask for feedback on the draft framework
- MS gave negative comments about the indicator's relevance for cybersecurity
- Lack of data or of Indicator's maturity or common understanding

The list of deleted/frozen indicators is in Annex I.

In addition, some sub-areas have been deleted and some indicators have been assigned to different sub-areas in order to achieve a balanced "impact" of each indicator on the EU-CSI.

[1] Frozen indicators are indicators for which data might become available in the future.

ANNEX I

List of indicators discarded with respect to the draft EU-CSI 2023 Pilot version presented earlier this year (frozen indicators in *italics*).

Discarded on the basis of low scoring by MS:

1. Share of surveyed essential/important entities covered by insurance
2. Share of enterprises covered by insurance
3. *Availability of cybersecurity professionals*
4. *Strategic cybersecurity innovation*

Discarded on the basis of negative comments about relevance for cybersecurity

5. Information security compliance GDPR - share
6. Information security compliance GDPR – cases
7. EU and MS-funded cyber capacity building projects in third countries (EU)
8. Engagement with other CSIRT(s)

Discarded due to lack of data/maturity/common understanding

9. National spending on cybersecurity R&D
10. Managerial approval of cyber baseline(s) in essential/ important entities
11. Certification capacity at national level
12. National cybersecurity awareness and cyber hygiene initiatives
13. Mechanism for national-level risk assessment
14. Number of organisations ISO certified

→ merged into: average percentage of organisations with any of the three ISO certificates (ISO 22301:2019; ISO 27001:2013; ISO 28000:2007)

ANNEX II – DETAILED LIST OF INDICATORS

Detailed list of indicators with areas, sub-areas, sources, links, and weighting are provided in the attached excel file.

ANNEX III – STATISTICAL MODEL OVERVIEW

The Index consists of **4 main areas** (Policy, Capacity, Market/Industry and Operations). Each area contains one or more subareas, while subareas are comprised of indicators. For the EU-CSI Index in 2023, **60 indicators** were used, divided in **16 subareas**.

The sources used to derive the data are:

Data Source	Description
ENISA survey	Input for 24 Indicators was requested from MS representatives
Eurostat	https://ec.europa.eu/eurostat/data/database
Eurobarometer	https://europa.eu/eurobarometer/screen/home
ENISA Project - CYBERHEAD	https://www.enisa.europa.eu/topics/education/cyberhead
ISO website	https://isotc.iso.org/livelink/livelink?func=ll&objId=21897526&objAction=browse&viewType=1
ENISA – NIS Investments study	https://www.enisa.europa.eu/publications/nis-investments-2021 https://www.enisa.europa.eu/publications/nis-investments-2023
ENISA Data from CIRAS tool	ENISA Internal Database - https://ciras.enisa.europa.eu/
Website of the Council of Europe	https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185
ENISA - CSIRTs by country map	https://www.enisa.europa.eu/topics/incidence-response/csirt-inventory/certs-by-country-interactive-map
ENISA - NIS Investments Report	https://www.enisa.europa.eu/publications/nis-investments-2022
EC - Horizon Dashboard	https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-dashboard

The index is calculated in a hierarchical way, as shown in Figure 1. 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.

Methodological Details

Data treatment: Outliers

Upon initial analysis, outliers were detected in the indicators based on two criteria:

1. Skew and Kurtosis: Absolute skewness > 2.0, kurtosis > 3.5 (or > 10 for kurtosis).
2. Interquartile Range (IQR): Defined as falling below Q1 - 1.5 IQR or above Q3 + 1.5 IQR.

Identified outliers led to the application of Winsorisation for treatment, replacing outliers with the nearest non-outlying values. This method is favoured when outliers are present in a small percentage (approx. 5%) of units. In our methodology, Winsorisation was chosen due to the relatively low number of outliers in each case.

For the survey indicators, we identified outliers, however we do not treat them as we want to reflect these variations to the Index, since these points are valid answers from the Member States.

Imputation of missing indicator values

In statistics, imputation is the process of replacing missing data with substituted values. In EU-CSI we had the following cases of missing data imputation:

- As described above, for 24 out of 60 indicators, the data was requested from MS. For each MS that answered, "*Data not available/Not willing to share*", we assigned a neutral score. The main idea was to assign a neutral score **half of the maximum total score** per question.
- For the indicators **Cybersecurity (curricula) graduates in higher education** and **Share of compromised IPs, services and servers** which had missing values for a few countries, the **unconditional median imputation** method was used (the missing value for a country was replaced by the median of the rest of the countries).

Normalization of indicator values

To aggregate indicators expressed in different units into the subareas and areas of the EU-CSI, they had to be normalised. In EU-CSI, normalisation was done using the min-max method, transforming the indicator values into a scale between 0 and 100. To ensure comparability over the years, assuming that the Index remains the same, during the normalization process instead of using this year's specific min and max values per indicator, we employed a global min-max approach with standardized targets. For indicators without a clear global minimum and maximum, we used 2023 minimum and maximum values.

Most indicators were designed to have a positive direction (i.e. where higher is better), except from Shodan indicators "Cyber-attack surface nationwide", "Vulnerability patching effectiveness" and "Share of compromised IPs, services and servers" which are inversed during normalisation.

Take for example indicator: **Enterprises: ICT security measures.** This indicator's **minimum value is equal to 0 and its maximum value is equal to** 100 since this indicator represents a share. If a country has a raw value of 45 in this indicator, its normalized value will be:

$$\mathbf{\frac{45-0}{100-0}=0.45}$$

We also scale this value to the interval [0,100] by multiplying by 100, resulting in the final normalised value **45%**.

Weights

For this year's EU-CSI, weights were applied only on the indicators' level. Each weight represents the average score across three criteria as analysed in section 3: **Impact of the indicator on an area**, **relevance for NIS2 implementation**, **relevance indicated in the feedback survey**.

For the indicators "SMEs: ICT Security Measures" and "SMEs: Staff Awareness", which were added after the feedback survey was completed, we use the average of the other two dimensions.