European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

2024 EUCSI FRAMEWORK OVERVIEW

1. SCOPE OF DOCUMENT

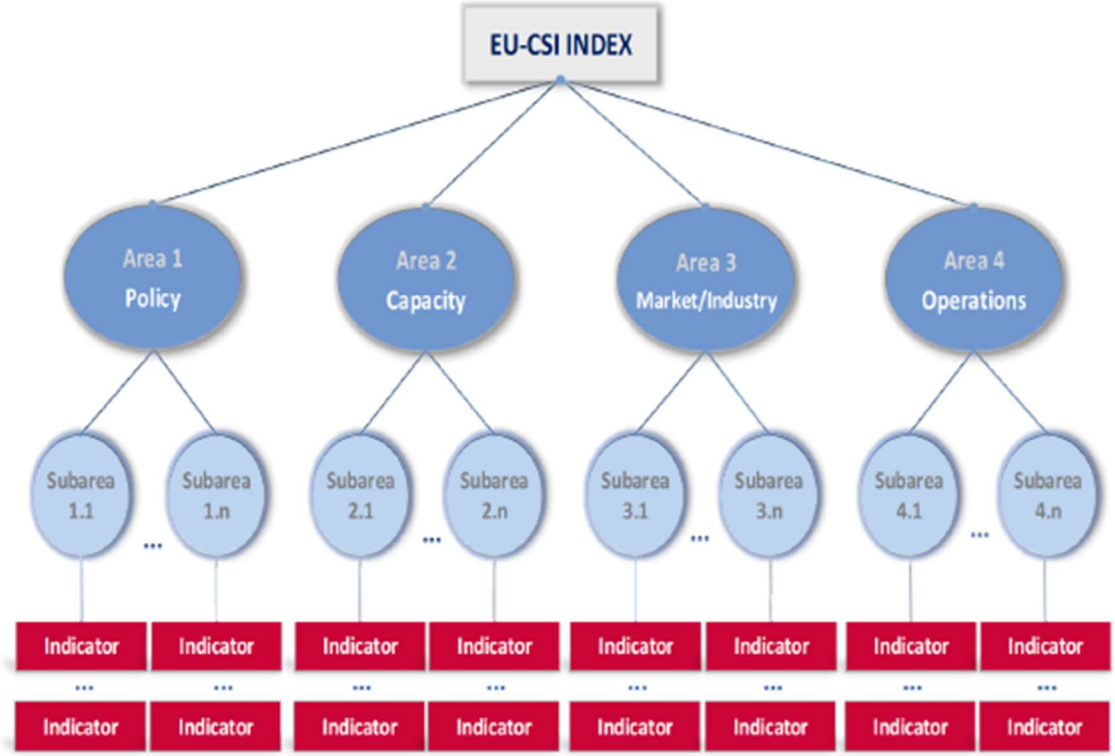
Since 2021 ENISA has been working on the development of a EU Cybersecurity Index, describing the cybersecurity posture of the EU and Member States (MS). ENISA has run the first pilot (EU-CSI 2022 Pilot), and the updated version for the following year (EU-CSI 2023).This document describes the updated version for the EUCSI 2024.

2. OVERVIEW OF THE 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:



The EU-CSI 2024 Index is composed by 60 indicators, structured hierarchically across 15 sub-areas and 4 areas.

The tables below show the areas and sub-areas of the Index. Each area and sub-area feature 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	This area describes the ability of society to recognise threats and prevent incidents.
Sub-areas	
Cyber hygiene Implementation of measures for cyber hygiene.	• Large enterprises: ICT security measures • Citizens: privacy and protection of personal data • Citizens: secure internet use • SMEs: ICT security measures
Cybersecurity awareness Knowledge and understanding of cybersecurity and efforts to increase cybersecurity awareness.	• Large enterprises: Staff Awareness • Citizens: Knowledge of cybersecurity matters • SMEs: Cybersecurity training • SMEs: Staff Awareness
Cybersecurity skills and education Availability of measures to increase specialised cybersecurity skills and knowledge.	• National level cybersecurity trainings • Tools and training to fight cybercrime • Cybersecurity exercises at national and international level • EU R&D funding • Cybersecurity graduates in higher education

Area: Market/Industry	This area describes the 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: risk assessment • Enterprises: ICT security policy • Organisations certified with relevant ISO standards • Supply chain management by essential/ important entities
Cybersecurity investments and innovation Extent to which enterprises invest into their current and future security.	• Cybersecurity investments by essential/important entities • Enterprises buying security software applications as a cloud computing service • Enterprises using AI technologies for ICT security • SMEs: EU R&D funding
Large enterprises: Impact of cybersecurity incidents Extent to which large enterprises have suffered from cybersecurity incidents.	• Large enterprises: Security Incidents - Destruction or corruption of data • Large enterprises: Security Incidents - Disclosure of confidential data • Large enterprises: Security Incidents - Unavailability of ICT Services
SMEs: Impact of cybersecurity incidents Extent to which SMEs have suffered from cybersecurity incidents.	• SMEs: Security Incidents - Destruction or corruption of data • SMEs: Security Incidents - Disclosure of confidential data

	• SMEs: Security Incidents - Unavailability of ICT Services

Area: Operations	**This area describes the ability of a MS 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 • CSIRT(s) certification
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 • CSIRTs international presence
Resilience of key operators Resilience of key operators in terms of incidents and their duration.	• Participation by essential and important entities in a national or EU-level ISAC • 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
Threat and vulnerability management Efforts for threat and vulnerability management	• Cyber-attack surface nationwide • Vulnerability patching effectiveness • Share of compromised IPs, services and servers • Use of secure internet standards

Area: Policy	**This area describes the state of policy development and implementation.**
Sub-areas	
Coverage and enforcement of legal and regulatory framework Existence and coverage of national cybersecurity legislations	• Coverage of essential sectors by national legislation • Coverage of vulnerability disclosure policies • Implementation of cybersecurity EU legislation • Coverage and implementation of objectives in national cybersecurity strategy
International cooperation Alignment with international practices and policies.	• Establishment of international cooperation mechanisms • International cooperation on cybersecurity • Alignment with the Council of Europe Convention on Cybercrime

National-level risk management Coverage of risk-management at 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
Policies for knowledge Definition of a policy framework for the development of cybersecurity knowledge.	• Cybersecurity in higher education • Cybersecurity in national education curricula • Cybersecurity in R&D priorities and initiatives • National and international cooperation for cybersecurity R&D

3. WEIGHTS

For the weights we follow the methodology defined last year. ENISA will use 3 dimensions to score each indicator and the average of those scores will be the indicator's weight.

The dimensions are:

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 NIS1/NIS2 implementation **Extent to which an indicator conveys information about a country's NIS2 transposition and implementation**	**Score 0-1**
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

For the first phase of the weights analysis, we were given the scores per dimension by ENISA and we calculated the weights of indicators. Due to the different scales of the dimensions, we first normalised the scores of the 3rd dimension using Min-Max normalisation, with minimum 1 and maximum 5, and bring all dimensions to 0-1 scale.

The dimensions scoring use for EU-CSI 2024 is the same used in 2023, except from the survey indicators, in which the **Relevance indicated in the feedback survey** dimension was updated using the indicator ranking of the Survey 2024 filled by the Member States.

Moreover, as a result of the multivariate analysis we performed, we made the following adjustments in the weighting schema:

- For CIRAS (except E-trust cases) and Shodan indicators, we have lowered their weights since we have identified some issues with these certain indicators. The dimensions' configuration we use for these indicators is MS relevance 1; NIS relevance: 0.5; impact on area: 0. Moreover, the reasoning for keeping the same weight for E-trust cases stems from the fact that we have corrected this indicator by using the number of certificates in the calculation.
- For the indicators "SMEs: ICT Security Measures" and "SMEs: Staff Awareness", we use the **relevance indicated in the feedback survey score** of their "twin" indicators "Large enterprises: ICT security measures" and "Large enterprises: Staff Awareness".

4. EU-WIDE INDICATORS

In addition to the indicators used to calculate the EU-CSI, a set of **22 "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.

Indicator name
Internet infrastructures - Sector Cybersecurity Criticality
Electricity - Sector Cybersecurity Criticality
Health - Sector Cybersecurity Criticality
Telecom - Sector Cybersecurity Criticality
Transport/Aviation - Sector Cybersecurity Criticality
Trust services - Sector Cybersecurity Criticality
Gas - Sector Cybersecurity Criticality
Oil - Sector Cybersecurity Criticality
Finance- Sector Cybersecurity Criticality
Rail - Sector Cybersecurity Criticality
Internet infrastructures - Sector Cybersecurity Maturity
Electricity - Sector Cybersecurity Maturity
Health - Sector Cybersecurity Maturity
Telecom - Sector Cybersecurity Maturity
Transport/Aviation - Sector Cybersecurity Maturity
Trust services - Sector Cybersecurity Maturity
Gas - Sector Cybersecurity Maturity
Oil - Sector Cybersecurity Maturity
Finance - Sector Cybersecurity Maturity
Rail - Sector Cybersecurity Maturity
Share of surveyed suppliers of cryptographic products with EU-based design and development
Average knowledge gap related to cryptographic product and services between the demand side and the supply side of such product/services

ANNEX – 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 **15 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.

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*", we assigned EU average per question rounded down to the lowest possible score. The main idea was to assign a score that will not "punish" countries that had not available data to share.
- For some indicators (Cybersecurity graduates in higher education and E-trust services resilience (e-IDAS) – cases), we had some null records in the variables that we use to calculate the final indicator values. For the CS graduates we have null values in the nominator (number of CS graduates), so in order not to favour/punish countries due to their size as far as population is concerned, we first calculate the indicator value and then we impute. For the E-trust cases, we have null values in the denominator (certificates), so in order not to lose the information on e-Trust cases we fist impute the number of certificates with the median and then perform the computation with the e-trust cases number of the country.

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 for most indicators, 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 structure 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 with small values by nature, for which we do not have a better target, we have either opted for the fraction to the maximum or the ranking normalisation process. The reasoning for selecting between these two approaches, is that, for the indicators that we know they express shares we use the fraction to the maximum (ISO, CS graduates indicators) and for those that express a rate or something different (Shodan, CIRAS indicators), we use the ranking normalisation. We note here that to retain comparability over the years, we will use 2024 maximum value as a baseline.

Take for example indicator: **Large 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:

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

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 third dimension **Relevance indicated in the feedback survey,** since its range is from 1 to 5, we had to perform normalisation to transform it to the same scale as the rest of the dimensions (0-1) and calculate the final weight per indicator.

For CIRAS (except E-trust cases) and Shodan indicators, we have lowered their weights since we have identified some issues with these certain indicators. The dimensions' configuration we use for these indicators is MS relevance 1; NIS relevance: 0.5; impact on area: 0. Moreover, the reasoning for keeping the same weight for E-trust cases stems from the fact that we have corrected this indicator by using the number of certificates in the calculation.

For the indicators "SMEs: ICT Security Measures" and "SMEs: Staff Awareness", we use the **relevance indicated in the feedback survey score** of their "twin" indicators "Large enterprises: ICT security measures" and "Large enterprises: Staff Awareness".