EU Cybersecurity Index - Pilot

**Fields marked with \* are mandatory.**

# General information

* Name
* Surname
* email
* Which country are you representing?  AT - Austria

 BE - Belgium  BG - Bulgaria  HR - Croatia  CY - Cyprus  CZ - Czechia  DK - Denmark  EE - Estonia  FI - Finland

 FR - France  DE - Germany  EL - Greece  HU - Hungary  IE - Ireland

 IT - Italy  LV - Latvia

 LT - Lithuania

 LU - Luxembourg  MT - Malta

 NL - Netherlands  PL - Poland

 PT - Portugal  RO - Romania

SK - Slovak Republic

 SI – Slovenia

 ES - Spain

 SE - Sweden

 ID127 - Other

Comments, if any:

# Coverage and objectives of the National Cybersecurity Strategy (NCSS)

*Background information*

## The indicator reuses the first question for each objective identified in the National Cybersecurity Assessment Framework (NCAF).

* **Which objective(s) do you cover in your current NCSS or do you plan to cover it in the next edition?**

**[Note: Multiple answers possible]**

 1. Develop national cyber contingency plans

 2. Establish baseline security measures

 3. Secure digital identity and build trust in digital public services

 4. Establish an incident response capability

 5. Raise user awareness

 6. Organise cyber security exercises

 7. Strengthen training and educational programmes

 8. Foster R&D

 9. Provide incentives for the private sector to invest in security measures

 10. Improve the cybersecurity of the supply chain

 11. Protect critical information infrastructure

 12. Address cybercrime

 13. Establish incident reporting mechanisms

 14. Balance security with privacy

 15. Establish a public-private partnership (PPP)

 16. Institutionalise cooperation between public agencies

 17. Engage in international cooperation (not only with EU MS)  All objectives above are covered in the current NCSS

Comments, if any:

# Cybersecurity included in the National Risk Assessment (NRA)

* **Is cybersecurity included in your National Risk Assessment?**

 Yes  No

Comments, if any:

# Emerging (cyber) technology threats are considered by the National Risk Assessment (NRA)

* **Level 1: Have studies (technical, operational, political) been performed on the field of cybersecurity threats related to emerging technologies?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 2). Otherwise go to the next indicator i.e. indicator 5 - Priority of Critical Information Infrastructures (CII) in the country's NCSS]

* **Level 2: Does the NRA of your country identify cybersecurity threats related to at least two of the emerging technologies listed below?**
  + Post Quantum Cryptography (PQC)
  + Quantum Cryptography (QC)
  + Artificial intelligence (AI)
  + Emerging autonomous transport and IoT in smart cars
  + Emerging robotics
  + Emerging e-Health (remote diagnostics, remote surgeries, IoMT, etc)
  + Space technology
  + Smart cities
  + Metaverse

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 3). Otherwise go to the next indicator i.e. indicator 5 - Priority of Critical Information Infrastructures (CII) in the country's NCSS]

* **Level 3: Does the NRA of your country include an action a national-level contingency plan addressing the cybersecurity threats associated to the considered emerging technologies?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 4). Otherwise go to the next indicator i.e. indicator 5 - Priority of Critical Information Infrastructures (CII) in the country's NCSS]

* **Level 4: Do you have sufficient people dedicated to crisis planning, look at the lessons learnt and implement changes plan addressing the cybersecurity threats associated to the considered emerging technologies?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 5). Otherwise go to the next indicator i.e. indicator 5 - Priority of Critical Information Infrastructures (CII) in the country's NCSS]

* **Level 5: Is there a process in place (meaning a process indicating timing, actors and actions) to review the plan addressing the cybersecurity threats associated to the considered emerging technologies?**

 Yes  No

 Don't know

Comments, if any:

# Priority of Critical Information Infrastructures (CII) in the country's NCSS

*Background information:*

## The indicator reuses the questions of the National Cybersecurity Assessment Framework (NCAF) Tool for Objective 8: Protect critical information infrastructures.

Note: It is necessary to reply to yes to all questions within a level to attain that level and to have access to the questions in the next level

* **Level 1: Do you cover the objective in your current NCSS or do you plan to cover it in the next edition?**

 Yes  No

 Don't know

* **Level 1: Is there a general understanding that CII operators contribute to national security?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 1 questions, go to the next batch of questions (Level 2 questions). Otherwise go to the next indicator i.e. indicator 6 - Cybersecurity baseline(s) or standard(s) for Operators of Essential Services (OES)]

* **Level 2: Do informal practices or activities exist that participate to reaching the objective in a non- coordinated manner?**

 Yes  No

 Don't know

* **Level 2: Did you define intended results, guiding principles or key activities of your action plan?**

 Yes  No

 Don't know

* **Level 2: Do you have a methodology to identify essential services ?**

 Yes  No

 Don't know

* **Level 2: Do you have a methodology for the identification of CIIs?**

 Yes  No

 Don't know

* **Level 2: Do you have a methodology to identify OES?**

 Yes

 No

 Don't know

* **Level 2: Do you have a methodology to identify digital service providers?**

 Yes  No

 Don't know

* **Level 2: Do you have one or more national authority providing oversight on critical information infrastructure protection and the security of network and information systems? e.g. as required per the NIS (2016/1148) Directive**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 2 questions, go to the next batch of questions (Level 3 questions). Otherwise go to the next indicator i.e. indicator 6 - Cybersecurity baseline(s) or standard(s) for Operators of Essential Services (OES)]

* **Level 3: Do you have an action plan that is formally defined and documented?**

 Yes  No

 Don't know

* **Level 3: Do you have an action plan with a clear resource allocation and governance?**

 Yes  No

 Don't know

* **Level 3: Have you implemented the NIS (2016/1148) Directive?**

 Yes  No

 Don't know

* **Level 3: Have you implemented the ECI (2008/114) Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection?**

 Yes  No

 Don't know

* **Level 3: Do you have a national registry for identified OES per critical sector?**

 Yes  No

 Don't know

* **Level 3: Do you have a national registry for identified digital service providers?**

 Yes  No

 Don't know

* **Level 3: Do you have a national risk registry for identified or known risks?**

 Yes  No

 Don't know

* **Level 3: Do you have a methodology to map CII dependencies?**

 Yes  No

 Don't know

* **Level 3: Do you deploy risk management practices to identify, quantify and manage risks related to CIIs at a national level?**

 Yes  No

 Don't know

* **Level 3: Do you engage in a consultation process to identify cross border dependencies?**

 Yes  No

 Don't know

* **Level 3: Do you have a single point of contact responsible for coordinating issues related to the security of network and information systems at national level and cross-border cooperation at Union level?**

 Yes  No

 Don't know

* **Level 3: Do you define baseline cybersecurity measures (mandatory or guidelines) for digital service providers and all sectors identified in Annex II of the NIS (2016/1148) Directive?**

 Yes  No

 Don't know

* **Level 3: Do you provide tools or methodologies to detect cyber incidents?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 3 questions, go to the next batch of questions (Level 4 questions). Otherwise go to the next indicator i.e. indicator 6 - Cybersecurity baseline(s) or standard(s) for Operators of Essential Services (OES)]

* **Level 4: Do you review your action plan regarding the objective to test its performance?**

 Yes  No

 Don't know

* **Level 4: Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?**

 Yes

 No

 Don't know

* **Level 4: Do you review and consequently update the list of identified OES at least every two years?**

 Yes  No

 Don't know

* **Level 4: Do you have a procedure to update the risk registry?**

 Yes  No

 Don't know

* **Level 4: Do you have other mechanisms in place to measure that the technical and organisational measures implemented by OES are appropriate to manage the risks posed to the security of network and information systems? e.g. regular cybersecurity audits, national framework for the implementation of standard measures, technical tools provided by the government such as detection probes or system- specific configuration review...**

 Yes  No

 Don't know

* **Level 4: Do you have other mechanisms in place to measure that the technical and organisational measures implemented by digital service providers are appropriate to manage the risks posed to the security of network and information systems? e.g. regular cybersecurity audits, national framework for the implementation of standard measures, technical tools provided by the government such as detection probes or system-specific configuration review...**

 Yes  No

 Don't know

* **Level 4: Do you review and consequently update the list of identified digital service providers at least every two years?**

 Yes  No

 Don't know

* **Level 4: Do you use a security certification scheme (national or international) to help OES and digital service providers identify secure ICT products? e.g. SOG-IS MRA in Europe, national initiatives…**

 Yes  No

 Don't know

* **Level 4: Do you use a security certification scheme or qualification procedure to assess service providers working with OES? e.g. service providers in the field of incident detection, incident response, cybersecurity audit, cloud services, smart cards…**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 4 questions, go to the next batch of questions (Level 5 questions). Otherwise go to the next indicator i.e. indicator 6 - Cybersecurity baseline(s) or standard(s) for Operators of Essential Services (OES)]

* **Level 5: Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?**

 Yes  No

 Don't know

* **Level 5: Do you create and update threat landscape reports?**

 Yes  No

 Don't know

* **Level 5: Depending on the latest developments in the threat landscape, are you able to onboard a new sector in your CIIP action plan?**

 Yes  No

 Don't know

* **Level 5: Depending on the latest developments in the threat landscape, are you able to adapt new requirements in your CIIP action plan?**

 Yes  No

 Don't know Comments, if any:

# Cybersecurity baseline(s) or standard(s) for Operators of Essential Services (OES)

* **Do you gather data about the compliance of Operators of Essential Services (OES) with nationally established cybersecurity baseline(s) or standard(s) e.g. ISO/IEC 27001/27002?**

 Yes  No

[If you answer Yes, go to the next question. Otherwise go to the next indicator i.e. indicator 7 Business continuity planning posture of essential entities in a country]

* **In 2021, what was the share of OES in your country that complied with nationally established cybersecurity baseline(s) or standard(s) e.g. ISO/IEC 27001/27002?**

 0-20%

 21-40%

 41-60%

 61-80%

 81-100%

 Not willing to share this information

Comments, if any

# Business continuity planning posture of essential entities in a country

* **Do you gather data about the business continuity plans of Operators of Essential Services (OES) in your country?**

 Yes  No

[If you answer Yes, go to the next question. Otherwise go to the next indicator i.e. indicator 8 Participation of Operators of Essential Services (OES) in a national-level Information Sharing and Analysis Center (ISAC)]

* **In 2021, what was the share of OES in your country that had a business continuity plan?**

 0-20%

 21-40%

 41-60%

 61-80%

 81-100%

 Not willing to share this information Comments, if any

# Participation of Operators of Essential Services (OES) in a national-level Information Sharing and Analysis Center (ISAC)

* **Do you gather data about the participation of Operators of Essential Services (OES) in national-level Information Sharing and Analysis Centers (ISACs)?**

 Yes  No

 My country does not have national-level ISACs

[If you answer Yes, go to the next question. Otherwise go to the next indicator i.e. 9 Implementation of general cybersecurity-related EU Directives]

* **In 2021, what was the share of OES in your country that was a member of at least one national-level ISAC?**

 0-20%

 21-40%

 41-60%

 61-80%

 81-100%

 Not willing to share this information Comments, if any

# Implementation of general cybersecurity-related EU Directives

*Background information*

*The indicator assess the status of implementation of general cybersecurity-related EU Directives. A certain percentage is assigned to each implementation stage:*

***100%*** *if the Directive is fully transposed (notification sent to the EC) and entered into force*

***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*

[Note: only one answer for Directive is allowed]

*Status of Implementation*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **100%**:  Directive transposed and entered into force | **70%**:  legislation transposed, entry into effect in the future | **40%**: national legislation covers Directive partially, full transposition pending | **0%:**  otherwise |
| **\*** Directive (EU) 2018/1972 establishing the European Electronic Communications Code (EECC) |  |  |  |  |
| **\*** Directive (EU) 2016/1148 on measures for a high common level of cybersecurity across the Union (NIS Directive) |  |  |  |  |
| **\*** Directive (EU)2014/54 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment (RED Directive) |  |  |  |  |

Comments, if any

# Coverage of sector-specific cybersecurity legislation

* **Please indicate whether your country has adopted national legislation covering the cybersecurity aspects of the following NIS sectors:**

Note: multiple choice is allowed

 Energy  Transport  Banking

 Financial market infrastructures  Health sector

 Drinking water supply and distribution  Digital infrastructure

 None of the above

Comments, if any

# Information security compliance General Data Protection Regulation (GDPR)

* **How many unique registered infringement cases concerning information security (GDPR articles 28, 32, 34, or 35-39) above 50.000 euro did you have in 2021?**
* **What was the share of the GDPR infringement cases concerning information security (GDPR articles 28, 32, 34, or 35-39) over the overall GDPR infringement cases in 2021?**

### Only values of at most 100 are allowed

%

Comments, if any

# Cybersecurity in primary and second level education

* **How many primary schools were present in your country in 2021?**

### Only values of at least 0 are allowed

* **How many primary schools in your country offered at least basic training in cybersecurity awareness in 2021?**

### Only values of at least 0 are allowed

* **How many secondary schools were present in your country in 2021?**

### Only values of at least 0 are allowed

* **How many secondary schools in your country offered at least basic training in cybersecurity awareness in 2021?**

### Only values of at least 0 are allowed

Comments, if any

# National level cybersecurity exercises

*Background:*

## The questions are a selection from the NCAF questions under Objective 6 “Organise cybersecurity exercises”.

* **Level 1: Do you conduct crisis exercises in other sectors (other than cybersecurity) at a national level or pan-European level?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 2). Otherwise go to the next indicator i.e. indicator 14 - National level cybersecurity trainings]

* **Level 2: Do you have a cybersecurity exercise program at the national level?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 3). Otherwise go to the next indicator i.e. indicator 14 - National level cybersecurity trainings]

* **Level 3: Do you involve all related authorities of public administration? (even if the scenario is sector- specific)**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 4). Otherwise go to the next indicator i.e. indicator 14 - National level cybersecurity trainings]

* **Level 4: Do you write after action reports/evaluation reports?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question (Level 5). Otherwise go to the next indicator i.e. indicator 14 - National level cybersecurity trainings]

* **Level 5: Do you have a lessons learnt analysis capacity for cyber (reporting processes, analysis, mitigation)?**

 Yes  No

 Don't know Comments, if any

# National level cybersecurity trainings

* **How many cybersecurity trainings (e.g. awareness raising against phishing, technical trainings on incident response) has the National Competent Authority (or another national-level body) organised in 2021 for public sector employees?**

### Only values of at least 0 are allowed

* **How many cybersecurity trainings (e.g. awareness raising against phishing, technical trainings on incident response..) has the National Competent Authority (or another national-level body) organised in 2021 for the general public?**

### Only values of at least 0 are allowed

* **How many cybersecurity trainings (e.g. awareness raising against phishing, technical trainings on incident response..) has the National Competent Authority organised in 2021 for its own staff?**

### Only values of at least 0 are allowed

Comments, if any

# Cybersecurity monitoring

* **Does your country have a means (e.g. dedicated tools, reports…) to monitor the current cybersecurity threat level at the national level?**

 Yes  No

 Don't know

[If you answer Yes, go to the next question. Otherwise go to the next indicator i.e. indicator 16 - Crisis response to major cyber incidents]

* **How often does your country monitor the current cybersecurity threat level at the national level?**

 24/7

 Daily  Weekly

 Monthly

 Monitoring is not systematic

[If you answer Yes, go to the next question. Otherwise go to the next indicator i.e. indicator 16 - Crisis response to major cyber incidents]

* **In case of need, is your country equipped to communicate the threat level automatically to:**

 Public institutions

 Operators of Essential Services  Public

 Other

 Not equipped

Comments, if any

# Crisis response to major cyber incidents

*Background information:*

## The indicator reuses the questions of the National Cybersecurity Assessment Framework (NCAF) Tool for Objective 13: Establish incident reporting mechanisms

## **Note: It is necessary to reply to yes to all mandatory questions within a level to attain that level and to have access to the questions in the next level**

* **Level 1: Do you cover the objective "Establish incident reporting mechanisms" in your current NCSS or do you plan to cover it in the next edition?**

 Yes  No

 Don't know

* **Level 1: Do you have informal information sharing mechanisms on cybersecurity incidents incidents between private organisations and national authorities?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 1 questions, go to the next batch of questions (Level 2 questions). Otherwise go to the next indicator i.e. indicator 17 Country readiness to deal with cybercrime]

* **Level 2: Do informal practices or activities exist that participate to reaching the objective in a non- coordinated manner?**

 Yes  No

 Don't know

* **Level 2: Did you define intended results, guiding principles or key activities of your action plan?**

 Yes  No

 Don't know

* **Level 2: Do you have an incident reporting scheme for all the sectors under the annex II of the NIS Directive?**

 Yes  No

 Don't know

* **Level 2: Have you implemented the notification requirements for telecommunication service providers in compliance with article 40 of the Directive (EU 2018/1972)? The Directive requires that Member States shall ensure that providers of public electronic communications networks or of publicly available electronic communications services notify without undue delay the competent authority of a security incident that has had a significant impact on the operation of networks or services.**

 Yes  No

 Don't know

* **Level 2: Have you implemented the notification requirements for trust services providers in compliance with article (19) of the eIDAS Regulation (Regulation (EU) No 910/2014)? The article (19) requires, among other requirements, that providers of trust services notify the supervisory body about significant incidents**

/breaches.

 Yes  No

 Don't know

* **Level 2: Have you implemented the notification requirements for digital service providers in compliance with article (16) of the NIS Directive? The article (16) requires that digital service providers notify the competent authority or national CSIRT without undue delay of any incident having a substantial impact on the provision of a service as referred to in Annex III that they offer within the Union.**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 2 questions, go to the next batch of questions (Level 3 questions). Otherwise go to the next indicator i.e. indicator 17 Country readiness to deal with cybercrime]

* **Level 3: Do you have an action plan that is formally defined and documented?**

 Yes

 No

 Don't know

* **Level 3: Do you have an action plan with a clear resource allocation and governance?**

 Yes  No

 Don't know

* **Level 3: Do you have a mandatory incident reporting scheme that is functioning in practice?**

Yes No

Don't know

* **Level 3: Is there a coordination/cooperation mechanism for incident reporting obligations regarding GDPR, NISD, article 40 (ex-art13a) and eIDAS?Level 3: Do you have the adequate tools to ensure the confidentiality and integrity of information shared via the various reporting channels?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 3 questions, go to the next batch of questions (Level 4 questions). Otherwise go to the next indicator i.e. indicator 17 Country readiness to deal with cybercrime]

* **Level 4: Do you review your action plan regarding the objective to test its performance?**

 Yes  No

 Don't know

* **Level 4: Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?**

 Yes  No

 Don't know

* **Level 4: Do you have a harmonised procedure for sectorial incident reporting schemes?**

 Yes  No

 Don't know

* **Level 4: Do you have an incident reporting scheme for sectors others than the ones under the NIS Directive?**

 Yes  No

 Don't know

* **Level 4: Do you measure the effectiveness of incident reporting procedures? e.g. indicators on incidents that have been reported through the appropriate channels, timing of the incident report…**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 4 questions, go to the next batch of questions (Level 5 questions). Otherwise go to the next indicator i.e. indicator 17 Country readiness to deal with cybercrime]

* **Level 5: Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?**

 Yes  No

 Don't know

* **Level 5: Do you create annual incidents report?**

 Yes  No

 Don't know

**\*Level 5: Are there any cybersecurity landscape reports in place or other kinds of analysis prepared by the entity that receives the incident reports?**

 Yes  No

 Don't know Comments, if any

# Country readiness to deal with cybercrime

*Background information:*

## The indicator reuses the questions of the National Cybersecurity Assessment Framework (NCAF) Tool for Objective 12: Address cybercrime

## **Note: It is necessary to reply to yes to all questions within a level to attain that level and to have access to the questions in the next level**

* **Level 1: Do you cover the objective "address cybercrime" in your current NCSS or do you plan to cover it in the next edition?**

 Yes  No

 Don't know

* **Level 1: Have you performed a study to identify the law enforcement requirements (legal basis, resources, skills…) to effectively address cybercrime?**

 Yes  No

 Don't know

* **Level 1: Have you performed a study to identify the prosecutors and judges requirements (legal basis, resources, skills…) to effectively address cybercrime?**

 Yes  No

 Don't know

* **Level 1: Has your country signed the Council of Europe Budapest Convention on Cybercrime?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 1 questions, go to the next batch of questions (Level 2 questions). Otherwise go to the next indicator i.e. indicator 18 Cybersecurity Research and Development (R&D)]

* **Level 2: Do informal practices or activities exist that participate to reaching the objective in a non- coordinated manner?**

 Yes  No

 Don't know

* **Level 2: Did you define intended results, guiding principles or key activities of your action plan?**

 Yes  No

 Don't know

* **Level 2: Is your national legal framework fully complying with the relevant EU legal framework, including the Directive 2013/40/EU on attacks against information systems? e.g. Illegal access to information systems, Illegal system interference, Illegal data interference, Illegal interception, Tools used for committing offences...**

 Yes  No

 Don't know

* **Level 2: Do you have any legal provision addressing online identity theft and personal data theft?**

 Yes  No

 Don't know

* **Level 2: Do you have any legal provision addressing online intellectual property and copyright infringements?**

 Yes  No

 Don't know

* **Level 2: Do you have any legal provision addressing online harassment or cyber-bullying?**

 Yes  No

 Don't know

* **Level 2: Do you have any legal provision addressing computer-related fraud? e.g. compliance with provisions the Council of Europe Budapest Convention on Cybercrime**

 Yes  No

 Don't know

* **Level 2: Do you have any legal provision addressing child online protection? e.g. compliance with provisions of Directive 2011/93/EU and the Council of Europe Budapest Convention on Cybercrime**.

 Yes  No

 Don't know

* **Level 2: Have you identified an operational national point of contact to exchange information and to answer urgent information requests from other Member States relating to offences set out in Directive 2013/40/EU (Directive on attacks against information systems)?**

 Yes  No

 Don't know

* **Level 2: Does your law enforcement agency include a dedicated cybercrime unit?**

 Yes  No

 Don't know

* **Level 2: Have you designated, in accordance with Art. 35. Budapest Convention, a 24/7 point of contact?**

 Yes  No

 Don't know

* **Level 2: Have you designated an operational 24/7 national point of contact for the EU Law Enforcement Emergency Response Protocol (EU LE ERP) to respond to major cyber-attacks?**

 Yes  No

 Don't know

* **Level 2: Do you provide specialised training to stakeholders involved in addressing cybercrime (LEAs, judiciary, CSIRTs) on a regular basis? e.g. training sessions on filing/prosecuting cyber-enabled crimes, trainings on collecting electronic evidence and ensuring integrity throughout the digital chain of custody and computer forensics, among others**

 Yes  No

 Don't know

* **Level 2: Has your country ratified/acceded the Council of Europe Budapest Convention on Cybercrime?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 2 questions, go to the next batch of questions (Level 3 questions). Otherwise go to the next indicator i.e. indicator 18 Cybersecurity Research and Development (R&D)]

* **Level 3: Do you have an action plan that is formally defined and documented?**

 Yes  No

 Don't know

* **Level 3: Do you have an action plan with a clear resource allocation and governance?**

 Yes  No

 Don't know

* **Level 3: Do you have units dedicated to handle cybercrime in prosecution offices?**

 Yes  No

 Don't know

* **Level 3: Do you have a dedicated budget allocated to cybercrime units?**

 Yes  No

 Don't know

* **Level 3: Have you established a central body/entity to coordinate the activities in the area of fighting cybercrime?**

 Yes  No

 Don't know

* **Level 3: Have you established cooperation mechanisms between relevant national institutions involved in fighting cybercrime, including law enforcement national CSIRTs?**

 Yes  No

 Don't know

* **Level 3: Do you cooperate and share information with other Member States in the area of fighting against cybercrime?**

 Yes  No

 Don't know

* **Level 3: Do you cooperate and share information with EU Agencies (e.g. Europol's EC3, Eurojust, ENISA) in the area of fighting against cybercrime?**

 Yes  No

 Don't know

* **Level 3: Do you have the adequate tools to address cybercrime? e.g. cybercrime taxonomy and classification, tools to collect electronic evidence, computer forensics tools, trusted sharing platforms...**

 Yes  No

 Don't know

* **Level 3: Do you have standard operating procedures to handle e-evidences?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 3 questions, go to the next batch of questions (Level 4 questions). Otherwise go to the next indicator i.e. indicator 18 Cybersecurity Research and Development (R&D)]

* **Level 4: Do you review your action plan regarding the objective to test its performance?**

 Yes  No

 Don't know

**\*Level 4: Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?**

 Yes  No

 Don't know

* **Level 4: Do you collect statistics following the provisions of article 14 (1) of Directive 2013/40/EU (Directive on attacks against information systems)?**

 Yes  No

 Don't know

* **Level 4: Do you collect separate statistics on cybercrime? e.g. operational statistics, statistics on cybercrime trends, statistics on cybercrime proceeds and induced damage…**

 Yes  No

 Don't know

* **Level 4: Do you evaluate the adequacy of the training provided to LEAs, judiciary and national CSIRT(s) personnel to address cybercrime?**

 Yes  No

 Don't know

* **Level 4: Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to cybercrime units within LEAs?**

 Yes  No

 Don't know

* **Level 4: Do you perform regular evaluations to ensure that you have sufficient resources (human, budget and tools) dedicated to cybercrime units within prosecution authorities?**

 Yes  No

 Don't know

* **Level 4: Do you have units dedicated courts or specialized judges to handle cybercrime cases?**

 Yes  No

 Don't know

* **Level 4: Do you have any dispositions dedicated to providing support and assistance to victims of cybercrimes (general users, SMEs, large companies)?**

 Yes  No

 Don't know

* **Level 4: Have you established an inter-institutional framework and cooperation mechanisms between all relevant stakeholders (e.g. LEA, national CSIRT, judiciary communities), including private sector (e.g. operators of essential services, service providers) where appropriate, to respond to cyber-attacks?**

 Yes  No

 Don't know

* **Level 4: Does your regulatory framework facilitate the cooperation between CSIRTs and LE?**

 Yes  No

 Don't know

* **Level 4: Do you have mechanisms in place (e.g. tools, procedures) to facilitate the information exchange and the cooperation between CSIRT/LE and possibly judiciary (prosecutors and judges) in the area of fighting against cybercrime?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 4 questions, go to the next batch of questions (Level 5 questions). Otherwise go to the next indicator i.e. indicator 18 Cybersecurity Research and Development (R&D)]

* **Level 5: Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?**

 Yes  No

 Don't know

* **Level 5: Do you have interinstitutional training or training workshops for LEAs, Judges, prosecutors and national/governmental CSIRTs at a national level and/or at a multilateral level?**

 Yes  No

 Don't know

* **Level 5: Do you participate in coordinated actions at international level to disrupt criminal activities? e.g. infiltration of criminal hacking forums, organised cybercrime groups, dark web markets and botnets takedowns…**

 Yes  No

 Don't know

* **Level 5: Is there clear segregation of duties across CSIRTs, LEAs and the judiciary (prosecutors and judges) when they cooperate for addressing cybercrimes?**

 Yes  No

 Don't know

* **Level 5: Does your regulatory framework facilitate the cooperation between CSIRTs/LE and judiciary (prosecutors and judges)?**

 Yes

 No

 Don't know

* **Level 5: Do you participate in building and maintaining standardised tools and methodologies, forms and procedures to be shared with EU stakeholders (LEAs, CSIRTs, ENISA, Europol's EC3…)?**

 Yes  No

 Don't know Comments, if any

# Cybersecurity Research and Development (R&D)

*Background information:*

## The indicator reuses the questions of the National Cybersecurity Assessment Framework (NCAF) Tool for Objective 8: Foster R&D

Note: It is necessary to reply to yes to all questions within a level to attain that level and to have access to the questions in the next level

* **Level 1: Do you cover the objective "Foster R&D" in your current NCSS or do you plan to cover it in the next edition?**

 Yes  No

 Don't know

* **Level 1: Have you performed studies or analyses to identify cybersecurity R&D priorities?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 1 questions, go to the next batch of questions (Level 2 questions). Otherwise go to the next indicator i.e. indicator 19 Country presence in the international cybersecurity arena]

* **Level 2: Do informal practices or activities exist that participate to reaching the objective in a non- coordinated manner?**

 Yes  No

 Don't know

* **Level 2: Did you define intended results, guiding principles or key activities of your action plan?**

 Yes  No

 Don't know

* **Level 2: Do you have a process to define R&D priorities (e.g. emerging topics for deterring, protecting, detecting, and adapting to new kinds of cyber attacks)?**

Yes  No

 Don't know

* **Level 2: Is the private sector involved in setting up R&D priorities?**

 Yes  No

 Don't know

* **Level 2: Is academia involved in setting up R&D priorities?**

 Yes  No

 Don't know

* **Level 2: Are there any national R&D initiatives related to cybersecurity?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 2 questions, go to the next batch of questions (Level 3 questions). Otherwise go to the next indicator i.e. indicator 19 Country presence in the international cybersecurity arena]

* **Level 3: Do you have an action plan that is formally defined and documented?**

 Yes  No

 Don't know

* **Level 3: Do you have an action plan with a clear resource allocation and governance?**

 Yes  No

 Don't know

* **Level 3: Is there a plan to link R&D initiatives with real economy?**

 Yes  No

 Don't know

* **Level 3: Are there any national projects related to cybersecurity in place?**

 Yes  No

 Don't know

* **Level 3: Do you have local/regional startup ecosystems and other networking channels (e.g. technological parks, innovation clusters, networking events/platforms) to foster innovation (including for cybersecurity startups)?**

 Yes  No

 Don't know

* **Level 3: Is there investment in cybersecurity R&D programs in academia and the private sector?**

 Yes  No

 Don't know

* **Level 3: Do you have industrial research chairs in universities to bridge research subjects and market needs?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 3 questions, go to the next batch of questions (Level 4 questions). Otherwise go to the next indicator i.e. indicator 19 Country presence in the international cybersecurity arena]

* **Level 4: Do you review your action plan regarding the objective to test its performance?**

 Yes  No

 Don't know

* **Level 4: Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?**

 Yes  No

 Don't know

* **Level 4: Are R&D cybersecurity initiatives in line with relevant strategic objectives, e.g. DSM, H2020, Digital Europe, EU cybersecurity strategy?**

 Yes  No

 Don't know

* **Level 4: Is there an evaluation scheme in place for R&D initiatives?**

 Yes  No

 Don't know

* **Level 4: Are there any cooperation agreements with universities and other research facilities?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 4 questions, go to the next batch of questions (Level 5 questions). Otherwise go to the next indicator i.e. indicator 19 Country presence in the international cybersecurity arena]

* **Level 5: Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?**

 Yes  No

 Don't know

* **Level 5: Do you pursue at a national level cooperation with any international R&D initiatives related to cybersecurity?**

 Yes

 No

 Don't know

* **Level 5: Are R&D priorities aligned with current or upcoming regulation (national level)?**

 Yes  No

 Don't know Comments, if any

# Country presence in the international cybersecurity arena

*Background information:*

## The indicator reuses the questions of the National Cybersecurity Assessment Framework (NCAF) Tool for Objective 17: Engage in international cooperation (not only with EU MS)

## **Note: It is necessary to reply to yes to all questions within a level to attain that level and to have access to the questions in the next level**

* **Level 1: Do you cover the objective "Engage in international cooperation (not only with EU MS)" in your current NCSS or do you plan to cover it in the next edition?**

 Yes  No

 Don't know

* **Level 1: Do you have an international engagement strategy?**

 Yes  No

 Don't know

* **Level 1: Do you have informal cooperation channels with other countries?**

 Yes  No

 Don't know

* **Level 1: Has public leadership expressed intention to engage in international cooperation in the field of cybersecurity?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 1 questions, go to the next batch of questions (Level 2 questions). Otherwise you can stop here]

* **Level 2: Do informal practices or activities exist that participate to reaching the objective in a non- coordinated manner?**

 Yes

No

 Don't know

* **Level 2: Did you define intended results, guiding principles or key activities of your action plan?**

 Yes  No

 Don't know

* **Level 2: Do you have cooperation agreements with other countries (bilateral, multilateral) or partners in other countries? e.g. information sharing, capacity-building, assistance…**

 Yes  No

 Don't know

* **Level 2: Do you have a single point of contact that can exercise a liaison function to ensure cross-border cooperation with Member State authorities (cooperation group, CSIRTs network…)?**

 Yes  No

 Don't know

* **Level 2: Do you have dedicated people involved in international cooperation?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 2 questions, go to the next batch of questions (Level 3 questions). Otherwise you can stop here]

* **Level 3: Do you have an action plan that is formally defined and documented?**

 Yes  No

 Don't know

* **Level 3: Do you have an action plan with a clear resource allocation and governance?**

 Yes  No

 Don't know

* **Level 3: Do you exchange information at strategic level? e.g. high-level policy, risk perception...**

 Yes  No

 Don't know

* **Level 3: Do you exchange information at tactical level? e.g. threat actors bulletin, ISACs, TTPs…**

 Yes  No

 Don't know

* **Level 3: Do you exchange information at operational level? e.g. operational coordination information, ongoing incidents, IOCs…**

 Yes  No

 Don't know

* **Level 3: Do you engage in international cybersecurity exercises?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 3 questions, go to the next batch of questions (Level 4 questions). Otherwise you can stop here]

* **Level 4: Do you review your action plan regarding the objective to test its performance?**

 Yes  No

 Don't know

* **Level 4: Do you review your action plan regarding the objective to ensure that it is correctly prioritised and optimised?**

 Yes  No

 Don't know

* **Level 4: Are national cybersecurity public agencies in your country involved in international cooperation schemes?**

 Yes  No

 Don't know

* **Level 4: Do you assess on a regular basis the outcomes of international cooperation initiatives?**

 Yes  No

 Don't know

[If you answer Yes to ALL Level 4 questions, go to the next batch of questions (Level 5 questions). Otherwise you can stop here]

* **Level 5: Do you have mechanisms in place to ensure that the action plan is dynamically adapted to environmental developments?**

 Yes  No

 Don't know

* **Level 5: Do you lead discussions on one or many topics within multilateral agreements?**

 Yes  No

 Don't know

* **Level 5: Do you lead discussions on one or many topics within international treaties or conventions?**

Yes

 No

 Don't know

* **Level 5: Do you lead discussions or negotiations in one or many topics within international groups of experts? e.g. The Global Commission on the Stability of Cyberspace (GCSC), ENISA NIS cooperation group, UN Group of Governmental Experts on Information Security (GGE)...**

 Yes  No

 Don't know Comments, if any