

The review of the Cybersecurity Act

Fields marked with * are mandatory.

Introduction

The 2025 Commission work programme has a strong focus on simplification to boost prosperity and resilience of the Union. This reflects the recommendation of [the Draghi report](#), which underlined that the accumulation of rules, complexity and challenges in implementing the rules are having a significant impact on Europe's competitiveness, limiting our economic potential and our prosperity. In this sense the Commission will propose [unprecedented simplification to boost prosperity and resilience, and to unleash opportunities, innovation and growth](#), launching a new drive to speed up, simplify and improve EU policies and laws, make rules clearer and easier to understand and faster to implement.

The revision of the [Cybersecurity Act](#) (Regulation (EU) 2019/881; the 'CSA'), which aims to achieve a high level of cybersecurity, cyber resilience and trust in the European Union, will be a cornerstone in this effort. In 2019, the CSA set a permanent mandate for the European Union Agency for Cybersecurity (ENISA) and established a European Cybersecurity Certification Framework (ECCF) for voluntary European cybersecurity certification schemes for information and communications technology (ICT) products, services and processes. From February 2025, the Cybersecurity Act, amended by [Regulation \(EU\) 2025/37](#), offers a possibility to request development of a certification scheme for managed security services under the ECCF as well.

In addition to reviewing the current aspects of the CSA, the revision of the Cybersecurity Act will be the driver for simplification of cybersecurity legislation. This includes measures to ensure more straightforward and more agile means to facilitate multiple-purpose reporting to avoid duplications. It will also address other ways to simplify cybersecurity rules. In that way, it will contribute to the broader simplification agenda of the Commission.

The review will also focus on the revision of ENISA's mandate, taking into account that since 2019, ENISA has been allocated additional tasks, by new cybersecurity legislation such as the [NIS2 Directive](#), the [Cyber Resilience Act](#), the [Cyber Solidarity Act](#) (CSoA), the [eIDAS Regulation](#) (as amended), the [Cybersecurity Regulation for EUIBAs](#) or the [Digital Operational Resilience Act](#) (DORA), or for example by the [European Action Plan on the cybersecurity of hospitals and healthcare providers](#). Similarly, the ECCF was tested in practice, as three

candidate schemes under the ECCF are presently in progress and the revision will look at an improved functioning of the ECCF. Considering lessons learnt from the functioning of ENISA and of the ECCF, the political commitment to simplification of EU legislation and current challenges in terms of cybersecurity that Member States, companies and organisations may face, this initiative aims to gather stakeholders' views on the following topics:

- **Section 1:** Mandate of ENISA.
- **Section 2:** European Cybersecurity Certification Framework.
- **Section 3:** Simplification of cybersecurity and incident reporting obligations.

This consultation is open to everybody: Member State competent authorities and regulators, cybersecurity organisations, EU bodies dealing with cybersecurity, trade associations and industry representatives, managed security service providers, researchers and academia, cybersecurity professionals, consumer organisations as well as non-governmental organisations and citizens.

You can upload a file with a more detailed contribution at the end of the questionnaire.

The consultation will remain open until 20th June 2025.

About you

* Language of my contribution

- ☐ Bulgarian
- ☐ Croatian
- ☐ Czech
- ☐ Danish
- ☐ Dutch
- ☒ English
- ☐ Estonian
- ☐ Finnish
- ☐ French
- ☐ German
- ☐ Greek
- ☐ Hungarian
- ☐ Irish
- ☐ Italian

- ☐ Latvian
- ☐ Lithuanian
- ☐ Maltese
- ☐ Polish
- ☐ Portuguese
- ☐ Romanian
- ☐ Slovak
- ☐ Slovenian
- ☐ Spanish
- ☐ Swedish

* I am giving my contribution as

- ☐ Academic/research institution
- ☒ Business association
- ☐ Company/business
- ☐ Consumer organisation
- ☐ EU citizen
- ☐ Environmental organisation
- ☐ Non-EU citizen
- ☐ Non-governmental organisation (NGO)
- ☐ Public authority
- ☐ Trade union
- ☐ Other

* First name

Diana

* Surname

Campar

* Email (this won't be published)

diana.campar@bdb.de

* Organisation name

255 character(s) maximum

* Organisation size

- ☐ Micro (1 to 9 employees)
- ☐ Small (10 to 49 employees)
- ☐ Medium (50 to 249 employees)
- ☒ Large (250 or more)

Transparency register number

Check if your organisation is on the transparency register. It's a voluntary database for organisations seeking to influence EU decision-making.

0764199368-97

Check if your organisation is on the [EU Transparency register](#). It's a voluntary database for organisations seeking to influence EU decision-making.

* Country of origin

Please add your country of origin, or that of your organisation.

This list does not represent the official position of the European institutions with regard to the legal status or policy of the entities mentioned. It is a harmonisation of often divergent lists and practices.

- | | | | |
|---|--|-------------------------------------|--|
| <input type="radio"/> Afghanistan | <input type="radio"/> Djibouti | <input type="radio"/> Libya | <input type="radio"/> Saint Martin |
| <input type="radio"/> Åland Islands | <input type="radio"/> Dominica | <input type="radio"/> Liechtenstein | <input type="radio"/> Saint Pierre and Miquelon |
| <input type="radio"/> Albania | <input type="radio"/> Dominican Republic | <input type="radio"/> Lithuania | <input type="radio"/> Saint Vincent and the Grenadines |
| <input type="radio"/> Algeria | <input type="radio"/> Ecuador | <input type="radio"/> Luxembourg | <input type="radio"/> Samoa |
| <input type="radio"/> American Samoa | <input type="radio"/> Egypt | <input type="radio"/> Macau | <input type="radio"/> San Marino |
| <input type="radio"/> Andorra | <input type="radio"/> El Salvador | <input type="radio"/> Madagascar | <input type="radio"/> São Tomé and Príncipe |
| <input type="radio"/> Angola | <input type="radio"/> Equatorial Guinea | <input type="radio"/> Malawi | <input type="radio"/> Saudi Arabia |
| <input type="radio"/> Anguilla | <input type="radio"/> Eritrea | <input type="radio"/> Malaysia | <input type="radio"/> Senegal |
| <input type="radio"/> Antarctica | <input type="radio"/> Estonia | <input type="radio"/> Maldives | <input type="radio"/> Serbia |
| <input type="radio"/> Antigua and Barbuda | <input type="radio"/> Eswatini | <input type="radio"/> Mali | <input type="radio"/> Seychelles |
| <input type="radio"/> Argentina | <input type="radio"/> Ethiopia | <input type="radio"/> Malta | <input type="radio"/> Sierra Leone |

- | | | | |
|--|---|--|--|
| <input type="radio"/> Armenia | <input type="radio"/> Falkland Islands | <input type="radio"/> Marshall Islands | <input type="radio"/> Singapore |
| <input type="radio"/> Aruba | <input type="radio"/> Faroe Islands | <input type="radio"/> Martinique | <input type="radio"/> Sint Maarten |
| <input type="radio"/> Australia | <input type="radio"/> Fiji | <input type="radio"/> Mauritania | <input type="radio"/> Slovakia |
| <input type="radio"/> Austria | <input type="radio"/> Finland | <input type="radio"/> Mauritius | <input type="radio"/> Slovenia |
| <input type="radio"/> Azerbaijan | <input type="radio"/> France | <input type="radio"/> Mayotte | <input type="radio"/> Solomon Islands |
| <input type="radio"/> Bahamas | <input type="radio"/> French Guiana | <input type="radio"/> Mexico | <input type="radio"/> Somalia |
| <input type="radio"/> Bahrain | <input type="radio"/> French Polynesia | <input type="radio"/> Micronesia | <input type="radio"/> South Africa |
| <input type="radio"/> Bangladesh | <input type="radio"/> French Southern and Antarctic Lands | <input type="radio"/> Moldova | <input type="radio"/> South Georgia and the South Sandwich Islands |
| <input type="radio"/> Barbados | <input type="radio"/> Gabon | <input type="radio"/> Monaco | <input type="radio"/> South Korea |
| <input type="radio"/> Belarus | <input type="radio"/> Georgia | <input type="radio"/> Mongolia | <input type="radio"/> South Sudan |
| <input type="radio"/> Belgium | <input checked="" type="radio"/> Germany | <input type="radio"/> Montenegro | <input type="radio"/> Spain |
| <input type="radio"/> Belize | <input type="radio"/> Ghana | <input type="radio"/> Montserrat | <input type="radio"/> Sri Lanka |
| <input type="radio"/> Benin | <input type="radio"/> Gibraltar | <input type="radio"/> Morocco | <input type="radio"/> Sudan |
| <input type="radio"/> Bermuda | <input type="radio"/> Greece | <input type="radio"/> Mozambique | <input type="radio"/> Suriname |
| <input type="radio"/> Bhutan | <input type="radio"/> Greenland | <input type="radio"/> Myanmar/Burma | <input type="radio"/> Svalbard and Jan Mayen |
| <input type="radio"/> Bolivia | <input type="radio"/> Grenada | <input type="radio"/> Namibia | <input type="radio"/> Sweden |
| <input type="radio"/> Bonaire Saint Eustatius and Saba | <input type="radio"/> Guadeloupe | <input type="radio"/> Nauru | <input type="radio"/> Switzerland |
| <input type="radio"/> Bosnia and Herzegovina | <input type="radio"/> Guam | <input type="radio"/> Nepal | <input type="radio"/> Syria |
| <input type="radio"/> Botswana | <input type="radio"/> Guatemala | <input type="radio"/> Netherlands | <input type="radio"/> Taiwan |
| <input type="radio"/> Bouvet Island | <input type="radio"/> Guernsey | <input type="radio"/> New Caledonia | <input type="radio"/> Tajikistan |
| <input type="radio"/> Brazil | <input type="radio"/> Guinea | <input type="radio"/> New Zealand | <input type="radio"/> Tanzania |
| <input type="radio"/> British Indian Ocean Territory | <input type="radio"/> Guinea-Bissau | <input type="radio"/> Nicaragua | <input type="radio"/> Thailand |
| <input type="radio"/> British Virgin Islands | <input type="radio"/> Guyana | <input type="radio"/> Niger | <input type="radio"/> The Gambia |
| <input type="radio"/> Brunei | <input type="radio"/> Haiti | <input type="radio"/> Nigeria | <input type="radio"/> Timor-Leste |
| <input type="radio"/> Bulgaria | <input type="radio"/> Heard Island and McDonald Islands | <input type="radio"/> Niue | <input type="radio"/> Togo |

- | | | | |
|--|-----------------------------------|--|--|
| <input type="radio"/> Burkina Faso | <input type="radio"/> Honduras | <input type="radio"/> Norfolk Island | <input type="radio"/> Tokelau |
| <input type="radio"/> Burundi | <input type="radio"/> Hong Kong | <input type="radio"/> Northern Mariana Islands | <input type="radio"/> Tonga |
| <input type="radio"/> Cambodia | <input type="radio"/> Hungary | <input type="radio"/> North Korea | <input type="radio"/> Trinidad and Tobago |
| <input type="radio"/> Cameroon | <input type="radio"/> Iceland | <input type="radio"/> North Macedonia | <input type="radio"/> Tunisia |
| <input type="radio"/> Canada | <input type="radio"/> India | <input type="radio"/> Norway | <input type="radio"/> Türkiye |
| <input type="radio"/> Cape Verde | <input type="radio"/> Indonesia | <input type="radio"/> Oman | <input type="radio"/> Turkmenistan |
| <input type="radio"/> Cayman Islands | <input type="radio"/> Iran | <input type="radio"/> Pakistan | <input type="radio"/> Turks and Caicos Islands |
| <input type="radio"/> Central African Republic | <input type="radio"/> Iraq | <input type="radio"/> Palau | <input type="radio"/> Tuvalu |
| <input type="radio"/> Chad | <input type="radio"/> Ireland | <input type="radio"/> Palestine | <input type="radio"/> Uganda |
| <input type="radio"/> Chile | <input type="radio"/> Isle of Man | <input type="radio"/> Panama | <input type="radio"/> Ukraine |
| <input type="radio"/> China | <input type="radio"/> Israel | <input type="radio"/> Papua New Guinea | <input type="radio"/> United Arab Emirates |
| <input type="radio"/> Christmas Island | <input type="radio"/> Italy | <input type="radio"/> Paraguay | <input type="radio"/> United Kingdom |
| <input type="radio"/> Clipperton | <input type="radio"/> Jamaica | <input type="radio"/> Peru | <input type="radio"/> United States |
| <input type="radio"/> Cocos (Keeling) Islands | <input type="radio"/> Japan | <input type="radio"/> Philippines | <input type="radio"/> United States Minor Outlying Islands |
| <input type="radio"/> Colombia | <input type="radio"/> Jersey | <input type="radio"/> Pitcairn Islands | <input type="radio"/> Uruguay |
| <input type="radio"/> Comoros | <input type="radio"/> Jordan | <input type="radio"/> Poland | <input type="radio"/> US Virgin Islands |
| <input type="radio"/> Congo | <input type="radio"/> Kazakhstan | <input type="radio"/> Portugal | <input type="radio"/> Uzbekistan |
| <input type="radio"/> Cook Islands | <input type="radio"/> Kenya | <input type="radio"/> Puerto Rico | <input type="radio"/> Vanuatu |
| <input type="radio"/> Costa Rica | <input type="radio"/> Kiribati | <input type="radio"/> Qatar | <input type="radio"/> Vatican City |
| <input type="radio"/> Côte d'Ivoire | <input type="radio"/> Kosovo | <input type="radio"/> Réunion | <input type="radio"/> Venezuela |
| <input type="radio"/> Croatia | <input type="radio"/> Kuwait | <input type="radio"/> Romania | <input type="radio"/> Vietnam |
| <input type="radio"/> Cuba | <input type="radio"/> Kyrgyzstan | <input type="radio"/> Russia | <input type="radio"/> Wallis and Futuna |
| <input type="radio"/> Curaçao | <input type="radio"/> Laos | <input type="radio"/> Rwanda | <input type="radio"/> Western Sahara |
| <input type="radio"/> Cyprus | <input type="radio"/> Latvia | <input type="radio"/> Saint Barthélemy | <input type="radio"/> Yemen |
| <input type="radio"/> Czechia | <input type="radio"/> Lebanon | <input type="radio"/> Saint Helena, Ascension and Tristan da Cunha | <input type="radio"/> Zambia |

- ☐ Democratic Republic of the Congo
- ☐ Lesotho
- ☐ Saint Kitts and Nevis
- ☐ Zimbabwe
- ☐ Denmark
- ☐ Liberia
- ☐ Saint Lucia

The Commission will publish all contributions to this public consultation. You can choose whether you would prefer to have your details published or to remain anonymous when your contribution is published. **For the purpose of transparency, the type of respondent (for example, 'business association', 'consumer association', 'EU citizen') country of origin, organisation name and size, and its transparency register number, are always published. Your e-mail address will never be published.** Opt in to select the privacy option that best suits you. Privacy options default based on the type of respondent selected

* Contribution publication privacy settings

The Commission will publish the responses to this public consultation. You can choose whether you would like your details to be made public or to remain anonymous.

☐ Anonymous

Only organisation details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published as received. Your name will not be published. Please do not include any personal data in the contribution itself if you want to remain anonymous.

☒ Public

Organisation details and respondent details are published: The type of respondent that you responded to this consultation as, the name of the organisation on whose behalf you reply as well as its transparency number, its size, its country of origin and your contribution will be published. Your name will also be published.









☒ I agree with the [personal data protection provisions](#)

Section 1: General questions on ENISA mandate

This section aims to introduce some general questions concerning the mandate of the European Union Agency for Cybersecurity (ENISA). The questions intend to gather information for the potential changes of the mandate and prioritization of tasks of ENISA, based on the related added value for stakeholders. The questions do not aim to assess ENISA's performance, which was subject to a previous evaluation exercise.

Current tasks of ENISA

Q1. Please provide your views regarding the importance of each of the current cybersecurity tasks entrusted to ENISA:

ENISA's task	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
* Development and implementation of Union policy and law (e.g., assisting Member States to implement Union policy and law, assisting Member States and Union institutions, bodies, offices and agencies in developing and promoting cybersecurity policies, etc.)					
* Building cybersecurity capacity (e.g., assisting in activities aiming at bolstering cybersecurity across the EU, etc.)					
* Operational cooperation at Union level (e.g., ENISA support for operational cooperation among Member States, EUIBAs and stakeholders, providing the secretariat of CSIRTs, assisting at the request of one or more Member States, in the assessment of incidents, etc.)					
* Market, cybersecurity certification, and standardisation (e.g., support and promote the development and implementation of Union policy on cybersecurity certification of ICT products, ICT services and ICT processes – monitoring developments, preparing candidate schemes, evaluating adopted schemes, standardisation and performing analyses of the main trends in the cybersecurity market, etc.)					
* Knowledge and information (e.g., perform analyses of emerging technologies, perform long-term strategic analyses of cyber threats and incidents, collect and analyse publicly available information about incidents, etc.)					

* Awareness-raising and education (e.g., raise public awareness of cybersecurity risks, organise regular outreach campaigns, promote cybersecurity education, etc.)					
* Research and innovation (e.g., contribute to the strategic research and innovation agenda)					
* International cooperation (e.g., contribute to the implementation of the Union's efforts when cooperating with third countries)					

Section 1.a. ENISA providing support in policy implementation

The following subsection aims to analyse a core task of the Agency, namely the support in cybersecurity policy implementation.

Q1. Where do you see the biggest added value of ENISA in the following suggestions:

ENISA's added value	Very important	Important	Somewhat important	Not very important	Do not know / No opinion
* Assisting Member States to implement Union policy and law regarding cybersecurity consistently. Examples include: issuing opinions and guidelines, providing advice and best practices on topics such as the European Cybersecurity Certification Framework, risk management, incident reporting and information sharing, etc.					
* Assisting the Commission with evidence-based information on the development and review of Union policy in the area of cybersecurity.					
* Support to industry (entities) in the form of best practices and technical guidance through reports/studies and analysis.					

* ENISA's contribution to the Union's efforts to **cooperate with key international partners**.



* **Q2. Do you see any other areas than those mentioned in Q1, where ENISA could bring big added value?**

Please, elaborate (with maximum 100 words):

The financial sector faces inconsistencies across Member States in incident reporting, causing high administrative burdens. ENISA's support could help harmonize practices, easing compliance and supporting the EU's simplification agenda. ENISA should not set regulations but play a technical and operational role in implementation. It could enhance cyber threat intelligence sharing, coordinate EU-level crisis responses, support regulatory coherence, and clarify responsibilities with national authorities. ENISA should also assist EU institutions in maintaining cybersecurity standards, develop sovereign tools like a European CVE database, and collaborate internationally to strengthen resilience against global cyber threats through strategic dialogue and shared best practices.

Section 1.b. ENISA providing technical support

Following the adoption of legislative acts such as the [NIS2 Directive](#), [Cyber Resilience Act](#), [Cyber Solidarity Act](#), [eIDAS Regulation on electronic identity and trust services](#), ENISA has received more specific technical tasks (establishing platforms, databases, templates, etc.) to support stakeholders in the implementation of EU law. ENISA will also establish a European Cybersecurity Support Centre for hospitals and healthcare providers, as set out in the [recent Action Plan](#) on the cybersecurity of hospitals and healthcare providers. This sub-section of the survey aims to gather more information on how the mandate of the Agency could address this set of specific services and their priority for stakeholders.

* **Q1. Do you consider that there should be additional technical tasks (apart from those included in the adopted legislative acts) that should be integrated in ENISA's mandate?**

- ☒ Yes
☐ No
☐ Do not know / no opinion

* If yes, please provide some examples:

Vulnerability coordination and management, Technical standardization and certification support, Advanced threat simulation and red-teaming, Real-time incident analysis and sharing, Supply chain cyber risk mapping.

* **Q2. Do you consider that ENISA is performing well in providing technical tasks (e.g. maintenance of platforms, databases and tools)?**

- ☐ Yes

- ☐ No
 - ☒ Do not know / no opinion
-

Section 1.c. ENISA's collaboration with other bodies

The cybersecurity ecosystem has evolved significantly since the last revision of ENISA's mandate in 2019. New actors are now part of the cyber fora and the relationship of the Agency with other stakeholders has evolved. This sub-section of the questionnaire aims to gather stakeholder views on ENISA's eventual involvement with other bodies.

*** Q1. Do you consider that ENISA's relationship and/or its partnership with other EU agencies, bodies, institutions etc. should be better specified in the founding act (the Cybersecurity Act)?**

- ☒ Strongly agree
 - ☐ Agree
 - ☐ Disagree
 - ☐ Strongly disagree
 - ☐ Do not know / no opinion
-

Section 1.d. ENISA's support in situational awareness

The following subsection aims to analyse a core task of the Agency, namely the support of ENISA in operational cooperation and gather stakeholders' views on operational cooperation and the situational awareness picture.

*** Q1: Pursuant to the current Article 7 of the Cybersecurity Act, ENISA supports the operational cooperation at Union level by creating synergies with other Union entities, organising cybersecurity exercises, contributing to a cooperative response to large-scale cyber incidents by providing a secretariat role for the CSIRTs Network and, within its framework, supporting Member States in capacity building, information sharing, analysis of vulnerabilities and incidents and, upon request, providing support in relation to ex post technical inquiries regarding significant incidents.**

In which areas defined in Article 7 should ENISA further strengthen its role? Which tasks, roles are no longer relevant? What new tasks, roles are important for ENISA to cover in the new mandate?

Please elaborate (with maximum 500 words):

We suggest that there should be an understanding of how the financial sector model with EU-SCICF interacts with everything else from ENISA as outlined in the question.

We would encourage a greater focus on information sharing, analysis of vulnerabilities and technical assistance. The current set of tasks is still relevant, however the role should be strengthened also in the light of international collaboration beyond the EU bodies.

In addition, the role of tests and training provided by ENISA to the member states and relevant organisations/ industry representatives should be strengthened.

Cybersecurity is increasingly important in our society and economy. If the current set of tasks of ENISA is still relevant, its role should be strengthened and evolve towards greater efficiency, practical support to stakeholders and coordination (especially beyond the EU bodies to avoid fragmentation and overtransposition). The recent development of the EUCS has demonstrated an opaque and siloed approach to decision-making. ENISA's works should be more transparent and accessible to national stakeholders and its reports should be rationalised for more simplification. Also, in the financial sector, the EU-SCICF forum is a place where relevant authorities communicate and coordinate actions when a systemic risk materialises. This EU-SCICF forum could take responsibility for operational cooperation and a cooperative response to large-scale cyber incidents with ENISA as an essential member. Indeed, the ECB Cyber Risk Stress Test likewise shows duplication in cyber exercises. We would encourage a greater focus on information sharing, analysis of vulnerabilities and technical assistance.

*** Q2: Should ENISA's role in supporting the constituency with capacity building be further strengthened (i.e. with specific support for ransomware prevention; sector specific support offered by ENISA; exercises organised by ENISA; challenges organised by ENISA)?**

- ☒ Yes
- ☐ No
- ☐ Do not know / no opinion

*** Q3: Do you think ENISA has a role to play in building a shared EU situational awareness picture together with other Union entities by providing relevant technical information?**

- ☒ Yes
- ☐ No
- ☐ Do not know / no opinion

Please elaborate (with max 100 words):

Smaller organisations often lack the resources to access and interpret global cybersecurity information. Beyond general guidance, information should be tailored by industry sector. If ENISA is to contribute to a shared EU-level situational awareness, this requires simplified procedures - especially in incident reporting and voluntary threat notifications. Situational awareness cannot rely solely on formal reports. Strengthened cooperation and direct dialogue with stakeholders are essential to ensure relevant, timely insights.

Section 1.e. ENISA and skills and awareness

The following subsection aims to analyse a core task of the Agency, namely the assistance of ENISA in awareness-raising and education, focusing more specifically on cyber skills.

Q1. To what extent do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
* ENISA should continue developing the European Cybersecurity Skills Framework (ECSF)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* ENISA should continue to coordinate EU-wide cyber awareness campaigns and challenges (e.g. European Cybersecurity Month, the European Cybersecurity Challenge...) and to develop guidance and tools addressing cybersecurity education and cybersecurity awareness (e.g. AR-in-a-Box, CyberEducation Platform, Cybersecurity Education Maturity Assessment, training material...)	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* ENISA should continue leading the work on developing an attestation scheme for cybersecurity skills, allowing ultimately for quality assurance and recognition of certifications in cybersecurity	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Section 2: Certification

This section is designed to explore key questions related to the European Cybersecurity Certification Framework (ECCF). The ECCF has a major role in strengthening cybersecurity to protect our industries, citizens and critical infrastructure against internal and external threats. Nevertheless, the evaluation of the Cybersecurity Act (CSA) has highlighted areas where improvements are needed, in particular as regards the adoption and governance process, the roles and responsibilities of the Member States, Commission and ENISA and the formalisation of the maintenance phase of the European cybersecurity certification schemes. Consequently, the questions in this section aim to collect insights to inform potential amendments to the ECCF, ensuring greater clarity, efficiency and stakeholder involvement.

Section 2.a. Scope, objectives, elements of schemes and harmonisation principle

Q1. What are the considerations, if any, that would encourage you to apply for a certificate under the European cybersecurity certification scheme?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
* Certification as means to improve the security of products or services	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Regulatory compliance, including presumption of conformity	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* International market access based on mutual recognition	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Reduction of legal exposure and potential financial liabilities	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Market or contractually required compliance	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Customer trust and credibility	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Reduction of administrative costs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Please elaborate your answer and list other considerations that would encourage you to apply for a certificate (with maximum 200 words):

A certificate is meaningful if we talk about high risk-relevant tools to provide regulatory certainty, security / quality assurance and trust. However, a certificate should not limit options, especially not innovation from abroad and/ or utilization of services from small innovative companies. We strongly favor no certificates for less security relevant products.

Certifications should in addition be mapped according to international standards or other certifications provided by equivalent jurisdictions. This can often define what certifications an institution may pursue and ENISA should consider mutual recognition more proactively.

*** Q2. What technologies / services or other related aspects would benefit from European cybersecurity certification in the next 5 to 10 years (e.g. IoT, crypto, PQC, physical security)?**

Please elaborate your answer (with maximum 100 words):

A certification for platform providers and systems on their Post Quantum Cryptography migration

A certification for Third Parties which provide AI Services. Main topics of the future are trust, sovereignty, secure supply chains, secure communication platforms, data driven regulatory-oversight. Hence, we need to focus on data systems, Cloud, IoT, quantum safe tech, G5.

Regarding the latter, a European cybersecurity certification that would enable firms to proactively confirm that they have completed an effective migration to Post Quantum Cryptography could be effective in demonstrating a high level of cyber maturity.

*** Q3. Do you consider that the scope, objectives and elements of the ECCF as expressed in the current CSA are clearly defined?**

- ☐ Strongly agree
- ☐ Agree
- ☒ Disagree
- ☐ Strongly disagree
- ☐ Do not know / no opinion

Please, elaborate your answer (with maximum 100 words):

The current objectives overlook cooperation with third-country agencies, despite the global nature of cyber threats. The EU should accelerate scheme development, align certification mandates with sectoral laws like DORA and NIS2, and create SME-friendly, cost-effective paths. Harmonization must reduce national overlaps and enable EU-wide recognition. Scope should expand to include governance, resilience, and privacy, with flexible assurance levels for complex use cases. International mutual recognition is essential to reduce duplication and boost competitiveness. Compliance with DORA already ensures sufficient assurance for digital products in banking, so the CRA should explicitly exclude these to avoid regulatory overlap and confusion.

*** Q4. Are there any elements that the European cybersecurity certification schemes should cover in addition to those currently foreseen in Article 54 of the [Cybersecurity Act](#) (i.e. assurance levels covered, evaluation criteria, vulnerability handling, content and format of certificates)?**

Please elaborate your answer (with maximum 100 words):

Any new certification scheme should assess existing EU regulations to avoid duplication. Under Article 54, it must identify frameworks offering equivalent assurance, such as DORA. For example, certification of payment cards under the CRA could overlap with DORA protections, requiring exemptions to prevent double regulation. Stronger post-certification monitoring, integration with DORA, NIS2, the AI Act, and the Data Act, and attention to emerging tech like AI and quantum cryptography are vital. Schemes must remain accessible to SMEs and proportionate. CRA should recognize equivalent safeguards in existing frameworks, as overlaps - particularly between CRA and DORA - create conflicting compliance obligations for financial services.

*** Q5. Do you think there are elements of the European cybersecurity certification schemes that could and should be harmonised for all European cybersecurity certification schemes (i.e. vulnerability handling, peer review mechanism, mark and label, scheme maintenance)?**

- ☒ Yes
- ☐ No
- ☐ Do not know / no opinion

* Please, elaborate your answer:

A mapping between the requirements of the various certification schemes (e.g. ISO 27001) would be useful.

* **Q6. Do you think European cybersecurity certification should be made mandatory for certain products / services / processes / managed security services?**

- ☐ Yes
- ☒ No
- ☐ Do not know / no opinion

* **Q7. Do you see a benefit in European cybersecurity certification that would be tailor-made to specific use-cases (products / services for specific industries)?**

- ☒ Yes
- ☐ No
- ☐ Do not know / no opinion

* Please, elaborate your answer (with maximum 100 words):

Tailored European cybersecurity certification offers clear benefits by addressing industry-specific risks and regulatory needs, improving relevance and effectiveness. It reduces compliance burdens and avoids unnecessary requirements, especially for SMEs, while ensuring alignment with sectoral laws like DORA. This fosters greater market trust and simplifies implementation, enabling faster, scalable adoption. Tailored schemes also support international recognition by aligning with global standards and encourage innovation by allowing flexible assurance for emerging technologies. Overall, industry-specific certifications provide clearer, more practical security assurance that better protects sectors and supports the EU's cybersecurity goals.

* **Q8: Do you see a benefit in incorporating personal data protection requirements in European cybersecurity certification to ensure synergy with data protection certifications under the [General Data Protection Regulation](#) (GDPR)?**

- ☐ Yes
- ☒ No
- ☐ Do not know / no opinion

Q9. To what extent do other recent EU legislations aimed at increasing the level of security of ICT products, ICT services and ICT processes, such as the

Cyber Resilience Act or the NIS2 Directive, impact the ECCF?

On a scale from 1 to 5 with 5 indicating to the very highest extent

4

Please, elaborate your answer (with maximum 100 words):

We support the Cyber Resilience Act's presumption of conformity for certified providers but oppose mandatory schemes due to significant overlap with DORA. DORA's comprehensive risk management framework covers all financial ICT services and grants regulators enforcement powers, overlapping with the ECCF's authority. CRA and NIS2 raise security baselines, increasing demand for certification and pressure for alignment to avoid duplication or conflicting requirements. CRA's inclusion of financial services in product certification overlaps with existing regulations like DORA, offering minimal cybersecurity benefits while granting market surveillance authorities new powers without financial regulator involvement.

Q10. Do you consider it useful to develop voluntary certification of entities that would support compliance with multiple cybersecurity and data security requirements of EU legislation (e.g. NIS2 Directive, DORA)?

On a scale from 1 to 5, with 5 indicating very useful

4

Section 2.b. Process of development and adoption of certification schemes

The following subsection aims to analyse the effectiveness, efficiency and transparency of the preparation and development of European cybersecurity certification schemes for ICT products, ICT services, ICT processes and managed security services in the Union for improving the functioning of the internal market.

Q1. Do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Do not know / No opinion
* The time needed to develop and adopt a European cybersecurity certification scheme is satisfactory.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* European cybersecurity certification schemes need to be regularly updated and amended.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* The process for the request, development and adoption of European cybersecurity certification schemes would benefit from increased transparency.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
*					

The Union Rolling Work Programme is an effective way of ensuring that industry, national authorities and standardisation bodies prepare in advance for the future European cybersecurity certification scheme (s).



Section 2.c. Governance of the certification framework

The questions in this subsection seek to gather views on potential changes to ENISA's mandate and prioritisation of its tasks within the ECCF including, but not limited to, preparation, development and maintenance of European cybersecurity certification schemes, thereby contributing to clarification of the roles and responsibilities.

Q1. What role do you consider ENISA should play in the following areas of the ECCF?

Statement	No role	Supporting role	Leading role	Do not know / No opinion
* Preparation / development of candidate schemes	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Maintenance of schemes: drafting of technical specifications	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Maintenance of schemes: organisation of ECCG subgroup meetings	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Guidance for application of schemes	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Promotion of the uptake of schemes	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Peer review mechanism	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Issuance of certificates for European cybersecurity certification schemes	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Testing and evaluation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
* Presumption of conformity with EU legislation	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

You may elaborate your answer(s) in the table (with maximum 100 words):

ENISA should provide technical leadership, harmonization oversight, stakeholder coordination, capacity building, and strategic foresight, serving as the ECCF's operational backbone and knowledge hub. However, it must avoid one-size-fits-all standards, respect proportionality, include industry input, and prevent duplication or conflicts with EU regulations. Key points include uniform certifications for major ICT providers to boost IT resilience, cloud provider certification under EUCS as an audit exemption, and facilitated access to security services without mandatory CSA certifications for low-risk institutions. Importantly, mandatory certification should be avoided for safety-critical hardware and software components to prevent reliance on outdated products.

Section 2.d. Stakeholder involvement

The questions in this subsection aim to collect additional insights to inform potential amendments to the framework to ensure greater and more streamlined stakeholder involvement, particularly in the preparatory, development and maintenance phases of European cybersecurity certification schemes.

*** Q1. Do you represent or have you in the past represented an organisation in the European Cybersecurity Certification Group (ECCG)?**

- ☐ Yes
- ☒ No
- ☐ Don't know / no opinion

*** Q2. How do you assess the level of effectiveness of the European Cybersecurity Certification Group?**

- ☐ Very low effectiveness
- ☒ Low effectiveness
- ☐ Medium effectiveness
- ☐ High effectiveness
- ☐ Very high effectiveness
- ☐ Do not know / no opinion

Q3. To what extent do you agree with the following statements regarding the ECCG?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
* The ECCG and the ECCF would benefit from more organised stakeholder interactions during preparatory stages of cybersecurity certification schemes.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* The role and tasks of the ECCG in the Cybersecurity Act are sufficiently clear.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* The ECCG has provided sufficient support to the Member States in the implementation of the ECCF.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* Member States should play a more active role in the governance of ECCG subgroups.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

*

Q4: Do you consider that the mandate of the ECCG should encompass additional tasks to those currently foreseen in the Cybersecurity Act?

The Cybersecurity Act outlines the tasks of the ECCG in Article 62(4), most prominently to advise and assist the Commission in its work to ensure the consistent implementation and application of the Title III of the Act.

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion

Please, specify which tasks (with maximum 100 words):

The ECCG mandate should include enhanced cross-sector coordination to address emerging threats, oversight of certification harmonization to prevent fragmentation, and development of sector-specific certification frameworks. It should support SMEs with simplified certification paths, establish post-certification monitoring and incident response, and promote international cooperation for mutual recognition. Additionally, the ECCG should provide strategic foresight by tracking emerging technologies like AI and quantum computing to anticipate future certification needs, ensuring the EU's cybersecurity framework remains adaptive and effective.

*** Q5. In your view, to what extent are relevant stakeholders sufficiently involved in the development of European cybersecurity certification schemes?**

- ☐ Not at all
- ☒ To a little extent
- ☐ To some extent
- ☐ To a high extent
- ☐ Do not know / no opinion

*** Q6. What other measures could be taken to further facilitate relevant stakeholders' participation?**

Please, elaborate (with maximum 100 words):

We urge a structured, regular multi-stakeholder dialogue that allows input early in the process, not just after draft schemes are developed. The public consultation should be more transparent and provide clear feedback on contributions. Simplified channels are needed for SMEs and startups to participate meaningfully, given the diverse industrial landscape. Previous consultations focused too narrowly on cloud providers, neglecting international perspectives and cloud users. Cloud sovereignty requirements risk conflicting with multilateral agreements and create legal complexities for financial institutions operating across jurisdictions, posing significant operational risks that must be addressed in consultation processes.

*** Q7. Is your organisation directly or indirectly (through association) part of the Stakeholder Cybersecurity Certification Group (SCCG)?**

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion

Q8. To what extent do you agree with the following statements regarding the SCCG?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
* The SCCG has sufficient opportunities to participate in ECCF.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* The SCCG actively contributes to the development of European cybersecurity certification schemes.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
* A single forum and governance mechanism with regular interactions with the ECCG, ENISA and the Commission could provide better opportunity for the group to fulfil its advisory role.	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Section 2.e. Supply chain security

Supply chain attacks have been identified as one of the seven prime cybersecurity threats by the [ENISA Threat Landscape 2024](#) report and cybersecurity risks associated with ICT supply chains have been justifiably given a lot of attention in recent years. The EU has taken multiple legislative initiatives to address supply chain security. In particular, Title III of the Cybersecurity Act sets out a framework for the development and adoption of the European cybersecurity certification schemes which provide assurance of the cybersecurity level of ICT products, services or processes that are used in the ICT supply chains. The [Directive \(EU\) 2022/2555](#) provides for an obligation on Member States to ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks. Such measures should cover supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers. The recently adopted Cyber Resilience Act introduces mandatory cybersecurity requirements for manufacturers and retailers to be met during the entire lifecycle of their products and at every stage of the supply chain.

*** Q1. In your view, during the last five years, how has the level of risk of cybersecurity incidents originating from ICT supply chains of entities operating in critical and highly critical sectors evolved?**

- ☐ Risk level has decreased significantly

- ☐ Risk level has decreased
- ☐ Risk level is the same
- ☒ Risk level has increased
- ☐ Risk level has increased significantly
- ☐ Don't know / no opinion

*** Q2: In your opinion what were the most common types of threats that led to ICT supply chain related cybersecurity incidents?**

Please, elaborate with maximum 100 words:

Insufficient cyber hygiene - such as unpatched and legacy systems - and social engineering attacks remain top threats. Compromise often stems from software dependencies, MSPs, and weak vendor security, worsened by poor supply chain visibility and inadequate third-party risk management. Software providers frequently rush releases without built-in security, leading to vulnerabilities like insecure authentication tokens, unauthorized privileged access, and opaque fourth-party dependencies. Providers must urgently prioritize security equally with product launches. "Secure and resilient by design" requires ongoing, demonstrable controls - not just annual compliance. Additional risks include service unavailability and data loss.

*** Q3. In your opinion, which sectors were the most affected by ICT supply chain incidents (please chose maximum 3)?**

between 1 and 3 choices

- ☐ Energy
- ☐ Transport
- ☐ Banking
- ☒ Financial markets infrastructures
- ☐ Health
- ☐ Drinking water
- ☐ Waste water
- ☐ Digital infrastructure
- ☒ ICT service management (managed security services)
- ☒ Public administration
- ☐ Space
- ☐ Postal and courier service
- ☐ Waste management
- ☐ Manufacture, production and distribution of chemicals
- ☐ Production, processing and distribution of food
- ☐ Manufacturing

- ☐ Digital providers
- ☐ Research

The Cybersecurity Act aims at achieving a high level of cybersecurity, cyber-resilience and trust within the Union, for which it addresses threats and risks related to network and information systems. Beyond technical factors, cybersecurity risks for ICT supply chains may also relate to non-technical factors such as undue influence by a third country on supplier (through for instance a strong link between the supplier and a government of a given third country, the third country's legislation, the supplier's corporate ownership or the ability for the third country to exercise any form of pressure on supplier). Such non-technical factors could pose unprecedented security challenges related to ICT supply chains that are currently not covered by the scope of the Cybersecurity Act.

*** Q4. Do you consider that there is a need to develop tools to address non-technical risks related to ICT supply chain security?**

- ☐ Strongly agree
- ☒ Agree
- ☐ Disagree
- ☐ Strongly disagree
- ☐ Do not know / no opinion

You may elaborate your answer (with maximum 100 words):

Technical tools alone won't solve ICT supply chain security. Transparency of dependencies and risks is essential for effective risk assessment, backup plans, and resilience strategies. Addressing supply chain security requires robust non-technical measures - improving governance, contracts, visibility, and overall resilience. Non-technical risks should not be managed through cybersecurity certifications but via targeted policy instruments to avoid unintended consequences like reduced market choice and resilience disruption. Existing policies, such as the Critical Third Party regime under DORA, specifically address these risks, particularly concerning non-EU providers, offering a more appropriate approach to managing supply chain challenges.

Q5. To what extent do you agree with the following statements?

Statement	Strongly disagree	Disagree	Agree	Strongly agree	Don't know / no opinion
* The application of organisational policies, processes and practices, including i.e. information sharing and vulnerability disclosure, in the area of cybersecurity risk management sufficiently mitigates all relevant risks related to the ICT supply chain security of entities.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

* Purely technical measures, such as the use of on-device processing, appropriate cryptography and other, can sufficiently mitigate all relevant risks related to the ICT supply chain security of hardware and software products.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
* The current European cybersecurity certification framework is an effective tool to facilitate cybersecurity safeguards for the public procurement of ICT products, ICT services and ICT processes.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Section 3: Simplification

This section aims to gather stakeholders' views as regards simplification of the cybersecurity legislation in line with the Commission's simplification agenda. It gathers the stakeholders' views as to whether incident reporting requirements and cybersecurity risk-management could potentially benefit from further simplification and streamlining, with the intended benefit of reducing unnecessary administrative burden.

* Q1. Which of the following EU pieces of legislation are/will be applicable to your entity/authority:

- ☒ Directive (EU) 2022/2555 (Network and Information Security Directive – **NIS2**)
- ☒ Regulation (EU) 2022/2554 (Digital Operational Resilience Act – **DORA**)
- ☒ Regulation (EU) 2024/2847 (Cyber Resilience Act – **CRA**)
- ☒ Directive (EU) 2022/2557 (Critical Entities Resilience Directive – **CER**)
- ☒ Regulation (EU) 2016/679 (General Data Protection Regulation – **GDPR**)
- ☒ Directive 2002/58/EC, as amended by Directive 2009/136/EC (**e-privacy Directive**)
- ☐ Commission Delegated Regulation (EU) 2024/1366 (Network Code on cybersecurity of cross-border electricity flows – **NCCS**)
- ☐ Aviation rules (Regulations (EC) No 300/2008 and (EU) 2018/1139 and the relevant delegated and implementing acts adopted pursuant to those Regulations)
- ☒ Regulation (EU) 2024/1689 (**AI Act**)
- ☒ Other

* Please, specify (with maximum 100 words):

PSD2, PSD3/PSR, eIDAS

Q2. Which of the following cybersecurity-related requirements laid down in the EU legislation referred to in Q1 ("relevant EU legislation") create or are likely to create in the near future the

biggest regulatory burden?

Please rate from 1 as the lowest burden to 6 as the highest burden

Different NIS2 incident reporting templates' formats, contents and procedures across the different EU Member States:

5

Different incident reporting tools/processes for relevant EU legislation at a national level:

5

Different incident reporting thresholds defining a reportable/significant /severe incident under the NIS2 Directive and across the different relevant EU legislations:

5

Implementation of cybersecurity risk-management measures stemming from relevant EU legislation:

5

Overlap of cybersecurity risk-management measures stemming from relevant EU legislation:

5

Requirements on how to prove implementation of cybersecurity risk-management measures ('compliance') stemming from relevant EU legislation:

5

Please explain and if possible, provide a quantification to the burden (with maximum 100 words):

The overlapping incident reporting requirements under DORA, NIS2, and the Cyber Resilience Act create significant burdens, especially for cross-border organizations. Multiple reports with fragmented procedures, formats, and definitions lead to duplicated efforts, tight deadlines, and high costs - often reaching millions annually in staff, systems, and legal expenses. This diverts resources from proactive security. Banks face particular challenges reporting to numerous authorities with inconsistent formats and unclear interplay between DORA and NIS2. A targeted simplification is urgently needed: a single, harmonized incident reporting process under DORA to reduce complexity, costs, and improve efficiency across the EU.

*** Q3. Do you consider that there are any other cybersecurity-related requirements laid down in relevant EU legislation not mentioned above that could be further streamlined?**

- ☒ Yes
☐ No
☐ I don't know / no opinion

*** Please, elaborate (with maximum 100 words):**

The need for targeted simplification on the Cyber Resilience Act and DORA. Furthermore, we need to have just one incident reporting under DORA and not also an extra one under NIS2 what makes the effort for us bigger to report.

- Harmonization of reporting timelines across regulatory frameworks
 - Development of a single comprehensive incident reporting regime
 - Reassessment of DORA reporting thresholds which currently trigger excessive reporting requirements
- If they are not directly cybersecurity-related requirements, financial sector regulations (PSD2/3 and PSR) need to be taken into account for a better streamline of incident reporting for banks (payment and cybersecurity incidents).

Q4. How effective do you consider the following solutions would be in removing administrative burden?

Please rate from 1 as the least effective to 6 as the most effective

Align reporting templates for NIS2 incident reporting of entities across all Member States:

6

Align reporting timelines for incident reporting across relevant EU legislation:

6

Align reporting requirements as regards content of reporting obligations across relevant EU legislation:

6

Introduce machine-readable standardised data formats for reporting across the EU:

6

Introduce one comprehensive set of rules for incident reporting in EU legislation:

6

Introduce a single reporting platform at national level for the compliance with reporting obligations stemming from relevant EU legislation:

6

Introduce a single reporting platform at EU level for the compliance with reporting obligations from NIS2:

6

Introduce a single reporting platform at EU level for the compliance with reporting obligations from all relevant EU legislation:

6

Introduce technical protocols and tools (such as APIs and machine-readable standards) for the purpose of automated reporting by entities to facilitate the integration of reporting obligations into business processes:

6

Align cybersecurity risk-management requirements stemming from relevant EU legislation:

6

Introduce one comprehensive set of rules for cybersecurity risk-management in EU legislation:

6

Introduce a higher level of harmonisation across specific sectors:

6

Please specify which sector (with maximum 20 words):

For Banking we see relevant harmonization needs with regards to NIS2, CRA, DORA, eIDAS, GDPR.

*** Q5. Would you suggest any other solutions to remove unnecessary administrative burden further to those mentioned above?**

- ☒ Yes
- ☐ No
- ☐ Don't know / no opinion

* Please, elaborate (with maximum 100 words):

We support EU-level simplification by stressing that sectoral regimes with equivalent protections should supersede horizontal ones, following the lex specialis principle seen between NIS2 and DORA. Similar treatment is urged for the Cyber Resilience Act due to significant overlaps. We also note reporting overlaps in the Digital ID and AI Acts, and testing overlaps with TIBER. Nationally, divergent incident reporting portals increase costs and delays; an EU-level hub could help but must be well-resourced and secure. Harmonization should leverage global convergence efforts, incorporating FSB FIRE and BCBS principles for third-party risk management in future revisions.

* **Q6. Would you agree for the Commission to potentially contact you for further discussion on simplification measures regarding cybersecurity legislation?**

- ☒ Yes
☐ No

* Please, fill in an email address and the name of your representative:

Critical areas requiring additional industry consultation:

- Operational impact of DORA incident reporting requirements
- Clarification of FIRE alignment mechanisms - Resolution of CRA/DORA regulatory duplication

diana.campar@bdb.de, Diana Campar on behalf of the German Banking Industry Committee (GBIC)

If you wish, please upload here a file with a more detailed contribution

Only files of the type pdf,doc,docx,odt,txt,rtf are allowed

Contact

EC-CNECT-CSA-REVIEW@ec.europa.eu

