Council of the European Union

Brussels, 21 January 2026
(OR. en)

5565/26
ADD 1

CYBER 24
JAI 84
DATAPROTECT 21
TELECOM 26
MI 56
IND 47
CADREFIN 25
FIN 99
BUDGET 2

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	20 January 2026
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	SWD(2026) 2 final
Subject:	COMMISSION STAFF WORKING DOCUMENT EVALUATION Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework

Delegations will find attached document SWD(2026) 2 final.

Encl.: SWD(2026) 2 final

EUROPEAN
COMMISSION

Brussels, 20.1.2026
SWD(2026) 2 final

COMMISSION STAFF WORKING DOCUMENT

EVALUATION

Accompanying the document

REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework

{COM(2026) 9 final}

Table of Contents

Table of Figures

GLOSSARY

The table below explains the key terms or acronyms used in this document.

Term or acronym	*Meaning or definition*
AI	Artificial intelligence
BEREC	Body of European Regulators for Electronic Communications
CAB	Conformity Assessment Body
CERT-EU	Cybersecurity Service for the Union institutions, bodies, offices and agencies
cPPP	Contractual Public-Private Partnership on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO) on 5 July 2016
CRA	Cyber Resilience Act
CSoA	Cyber Solidarity Act
CSA	Cybersecurity Act
CSIRT	Computer Security Incident Response Team
DORA	Digital Operational Resilience Act
EC	European Commission
EC3	European Cybercrime Centre
ECA	European Court of Auditors
ECCC	European Cybersecurity Competence Centre and Network
ECCF	European Cybersecurity Certification Framework
ECCG	European Cybersecurity Certification Group
EDA	European Defence Agency
eID	European Digital Identity
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
ENISA	European Union Agency for Cybersecurity
EU Cyber Blueprint	Council Recommendation on an EU blueprint for cyber crisis management (COM/2025/66 final)
EUCC	European Common Criteria
Europol	European Union Agency for Law Enforcement Cooperation
FTE	Full-time equivalent
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
IA	Impact assessment
ICT	Information and communication technologies
IoT	Internet of things

Term or acronym	*Meaning or definition*
ISAC	Information Sharing and Analysis Centre
MoU	Memorandum of Understanding
MS	Member State
NATO	North Atlantic Treaty Organization
NCC	National Coordination Centre
NGO	Non-governmental organisation
NIS	Network and information security
NIS2 Directive	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148
OECD	Organisation for Economic Cooperation and Development
PART-IS	EU Regulation on Information Security (PART-IS, Regulation (EU) 2023/203)
SCCG	Stakeholder Cybersecurity Certification Group
SME	Small and medium-sized enterprise
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
TFEU	Treaty on the Functioning of the European Union
URWP	Union rolling work programme

1. INTRODUCTION

The impact assessment (IA) report that accompanied the proposal for the Cybersecurity Act (CSA) in 2017[1] ('2017 IA') was developed by the European Commission to provide a comprehensive and evidence-based foundation for developing legislation on EU cybersecurity. The main purpose of the 2017 IA was twofold: (i) to assess whether the existing mandate and operations of the European Union Agency for Network and Information Security (ENISA) remained fit for purpose in a rapidly evolving threat and policy landscape, and (ii) to determine the need for an EU-wide cybersecurity certification framework for ICT products and services. The 2017 IA was not only a legal requirement under the then ENISA Regulation[2] but also a response to the growing recognition that cyber threats were increasing in scale and complexity and that fragmented national approaches to cybersecurity and certification risked undermining both the internal market and the EU's collective resilience.

Purpose and scope of the evaluation

Building on the 2017 IA, this evaluation report examines the performance of ENISA and the European cybersecurity certification framework (ECCF) since the adoption of the CSA. The evaluation was conducted in accordance with Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides the legal basis for EU action in this area, aiming to harmonise the laws of the Member States to ensure the proper functioning of the internal market. The internal market legal basis for ENISA has been recognised by the Court of Justice (C-217/04, judgment of 2 May 2006) and was further confirmed by the 2013 ENISA Regulation setting out ENISA's current mandate. Activities aimed at increasing cooperation and coordination and EU-level capabilities to complement the action of Member States fall within the field of operational cooperation. This is specifically identified by the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (hereafter referred to as NIS Directive), for which Article 114 TFEU is the legal basis. The Directive identifies operational cooperation as an objective to be pursued by the Computer Security Incident Response Team Network (CSIRTs Network), with ENISA providing the secretariat and actively supporting cooperation (Article 12(1)). Article 12(f) further identifies the following as tasks of the CSIRT Network: identifying further forms of operational cooperation, including in relation to categories of risks and incidents, early warnings, mutual assistance and principles and modalities for coordination when Member States respond to cross-border risks and incidents. Article 11(3) under the NIS2 Directive[3] also confirms this.

[1] Commission Staff Working Document Impact Assessment (2017) accompanying the proposal for a Regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency' and repealing Regulation (EU) 526/2013 and on information and communication technology cybersecurity certification ('Cybersecurity Act').

[2] Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance) (http://data.europa.eu/eli/reg/2013/526/oj).

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance) (http://data.europa.eu/eli/dir/2022/2555/oj).

The 2017 IA covered the performance, governance and organisational structure of ENISA, focusing on the period from 2013 to 2016, also taking into account more recent developments and anticipated future needs. The 2017 IA examined ENISA's support to Member States, its role in policy development and capacity building, its contribution to operational cooperation and its visibility and added value at both national and EU levels. In parallel, the IA addressed the emerging challenge of cybersecurity certification. It analysed the proliferation of national schemes, the lack of mutual recognition and the resulting risks of market fragmentation and increased compliance costs for businesses, particularly SMEs. The 2017 IA thus considered not only the effectiveness of ENISA's existing mandate but also the potential benefits and design of an ECCF.

This evaluation assesses the extent to which the objectives of ENISA's mandate and of the ECCF have been achieved, the effectiveness and efficiency of the measures implemented, their continued relevance, coherence with other EU policies and the added value of EU action. The evaluation addresses the main issues arising from the evolving cybersecurity landscape, such as the increasing number and sophistication of cyberattacks, the need for a high common level of cybersecurity across the EU and the fragmentation of certification schemes for ICT products and services.

In line with the European Commission's Better Regulation Guidelines, the evaluation applies all five compulsory criteria:

- **Relevance:** Examining whether the action continues to address the needs of stakeholders in light of technological and threat developments.
- **Effectiveness:** Assessing the extent to which the objectives of the existing framework have been achieved.
- **Efficiency:** Evaluating whether the resources invested are justified by the results obtained.
- **Coherence:** Analysing both internal coherence across the various provisions of the CSA, including ENISA's mandate and the ECCF, and external coherence in relation to other EU legislation such as Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, later replaced by Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS1 & NIS2 Directive), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (the General Data Protection Regulation or GDPR), Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation), and sectoral rules.
- **EU added value:** Considering whether action at EU level provides benefits that could not be achieved by Member States acting alone, particularly in terms of reducing fragmentation and supporting the functioning of the internal market.

The methodology for this evaluation combines a review of legal and policy documents, ENISA's annual reports and technical studies, along with other grey literature, with both quantitative and qualitative data analysis. The evidence base is further strengthened by stakeholder consultation, a call for evidence, targeted surveys, interviews and workshops

involving public authorities, EU institutions, industry, academia, civil society and individual citizens. Where possible, the assessment benchmarks EU approaches against international best practices and considers the coherence of measures with other relevant policies.

Despite its broad evidence base, the evaluation has several limitations. Data gaps persist in certain areas, particularly regarding the uptake and impact of certification schemes and the experiences of small and medium enterprises (SMEs) and end-users. The dynamic nature of the cybersecurity landscape and the concurrent evolution of related EU policies make it challenging to decide whether to attribute observed impacts solely to ENISA or to the certification framework. Furthermore, the representativeness of some stakeholder consultations is limited by the relatively low participation of certain groups.

The evaluation covers the period between 2019 and 2023. More recent developments, such as the Cyber Resilience Act (Regulation (EU) 2024/2847), could only partly be considered. The geographical scope includes all EU Member States, as well as countries participating in relevant EU cybersecurity initiatives, such as those in the European Economic Area and the European Free Trade Association and Horizon 2020-associated countries. The methodology and its limitations are described in detail in Annex II to the evaluation report.

2. WHAT WAS THE EXPECTED OUTCOME OF THE INTERVENTION?

This Chapter introduces the EU's action on cybersecurity as it falls within the scope of this evaluation, outlining its objectives, logic and the baseline conditions that shaped its design. The chapter explains how the CSA and the establishment of ENISA's mandate and the ECCF were intended to address persistent fragmentation, inconsistent protection and market barriers across Member States, based on the 2017 IA. By reconstructing the state of play prior to the CSA, this chapter provides the necessary context for evaluating the effectiveness and impact of the action in subsequent sections.

2.1 Description of the intervention and its objectives

The CSA, adopted in 2019, was designed to address persistent fragmentation and insufficient coordination in the EU's approach to cybersecurity. The preceding IA identified the need for a more coherent EU-wide approach, as existing legislation such as the NIS Directive, GDPR and eIDAS Regulation had resulted in a patchwork of national policies and certification schemes. This fragmentation undermined both the resilience of the internal market and the competitiveness of European industry.

The preferred options were a 'reformed ENISA' (Option 2) and the establishment of an EU general ICT security certification framework (Option 3). The explanatory memorandum confirms that these options were fully taken on board in the final CSA. ENISA was granted a permanent mandate and a central role in the EU cybersecurity ecosystem, with expanded responsibilities to support policy implementation, capacity building, support for operational cooperation and certification. The CSA also established the ECCF, aiming to harmonise certification schemes across the EU, reduce costs and administrative burdens and increase trust in ICT products, processes and services.

These actions were intended to address several interrelated problems. Fragmentation of cybersecurity policies and national certification schemes across Member States led to inconsistent levels of protection and market barriers. There were also dispersed resources and approaches among EU institutions, agencies and bodies, as well as insufficient awareness and information among citizens and businesses regarding cyber threats and the security properties of ICT products and services.

To tackle these problems, the following objectives were agreed upon:

- increase capabilities and preparedness of Member States and businesses,
- improve cooperation and coordination across Member States and EU institutions, agencies and bodies
- enhance EU-level operational capacity, particularly in the case of cross-border cyber crises
- raise awareness of cybersecurity issues among citizens and businesses,
- increase transparency of cybersecurity assurance for ICT products, services and processes and
- avoid further fragmentation of certification schemes and related requirements across the EU.

At the time of adoption, the expected achievements were clear. The CSA was expected to deliver a more harmonised and resilient cybersecurity landscape, with ENISA acting as a centre of expertise, supporting policy implementation, capacity building and operational cooperation. The ECCF was expected to streamline certification processes and reduce

costs by up to 80% for certain products. The intervention logic was that by empowering ENISA and establishing a harmonised certification framework, the EU would be better equipped to respond to cyber threats, support the digital single market and protect citizens and businesses. Success was expected to be reflected in a more harmonised and resilient cybersecurity landscape, with reduced costs and barriers for businesses and increased trust and awareness among users.

The strategic objective of the intervention logic for the EU cybersecurity certification scheme was formulated as follows: Create a European ICT Security Certification Framework that at the same time, avoids the fragmentation resulting from different approaches across European Union and is as close as possible up to international standards in order to reduce trade hindrances.

Quantitatively, according to the 2017 IA, before action was taken, certification costs for products like smart meters could exceed EUR 300 000 for two markets, with processes taking six to eighteen months. For cloud services, compliance costs were estimated at EUR 1.2 billion, representing up to 10% of annual expenditures and certification could take up to nine months. The CSA aimed to reduce these costs by up to 80% for smart meters and to achieve yearly savings of EUR 1.1 billion in the EU public sector for cloud services, with certification times reduced to four to six months.

2.2 Point(s) of comparison

This section reconstructs the state of play in the EU as of 2017, drawing on the 2017 IA and its supporting studies, stakeholders' consultations and economic analyses. The baseline scenario reflects the situation before the adoption of the CSA and serves as the main point of comparison for assessing subsequent developments. It covers ENISA's status and resources, the certification landscape, relevant market and economic data, as well as stakeholder perceptions and consultation data.

ENISA's status and resources

In 2017, ENISA was operating under a fixed-term mandate that was due to expire in 2020. Its annual EU contribution was EUR 10.3 million and it had an authorised establishment plan of 48 staff members, making it one of the smallest EU agencies in terms of both budget and personnel. Despite its broad mandate, which included support for policy development and implementation, capacity building, community building and support for operational cooperation, ENISA's resources were widely recognised as insufficient to meet the growing and evolving demands from Member States, EU institutions and the private sector.

When ENISA's performance was evaluated for the period 2013-2016, it was found to be relevant and efficient to a large extent, but its effectiveness, coherence and EU added value were only partially achieved. The fixed-term mandate was a significant limitation, as it prevented long-term planning and sustainable support for Member States and EU institutions. Furthermore, ENISA's ability to recruit and retain highly qualified experts was hampered by its location (split between Athens and Heraklion) and the predominance of fixed-term contracts, which made it less attractive compared to other agencies or the private sector.

Stakeholder consultations reinforced these findings. A majority of respondents considered ENISA's size insufficient for its workload. There was a broad consensus that both its resources and mandate needed to be adapted to enable it to support Member States in facing

future cybersecurity challenges. While ENISA's activities were generally coherent with those of other organisations, there was a clear need for a more coordinated approach at EU level. The agency's main added value was seen in its ability to enhance cooperation between Member States and communities under the NIS Directive, but its impact was limited by its scale and temporary mandate.

Certification landscape

The certification landscape in the EU in 2017 was highly fragmented and complex. Multiple national and sectoral certification schemes existed. Manufacturers often had to certify the same product multiple times to access different national markets. For example, according to the 2017 IA[4], smart meter manufacturers faced costs of around EUR 1 million to certify products in three countries, a barrier particularly penalised SMEs.

The SOG-IS Mutual Recognition Agreement (MRA) was the main European mechanism for certification, but it only included 12 Member States plus Norway and was limited to a few protection profiles for certain digital products. Certification processes were lengthy and costly: a CC certificate for the lowest assurance level could take six months and cost EUR 20 000, while higher assurance levels could take up to two years and cost at least EUR 500 000. The lack of a harmonised approach led to significant market fragmentation, increased costs and barriers to entry, especially for smaller companies.

Surveys conducted as part of the 2017 IA showed that a majority of respondents were aware of multiple certification schemes for the same product or service and a large majority agreed that mutual recognition was desirable at European level. The absence of a common EU framework for certification was widely seen as a major obstacle to the development of the digital single market and the competitiveness of European industry.

Relevant market and economic data

According to the 2017 IA, the economic impact of cybercrime in the EU was substantial. It was estimated at 0.41% of GDP, or around EUR 55 billion in 2013, with Germany being the most affected Member State (1.6% of GDP)[5]. The cost of certification for smart meters was at least EUR 300 000 for two markets and for cloud services, compliance costs were estimated at EUR 1.2 billion, representing 2% to 10% of companies' annual expenditure. Certification processes for cloud services could take 7-9 months.

The EU's investment in cybersecurity was below the critical mass needed to protect the economy and institutions, especially when compared to international competitors. For example, the US government invested over EUR 19 billion in cybersecurity in 2017, a 35% increase from 2016[6]. EU funding for cybersecurity projects under Horizon 2020 was about EUR 600 million for 2013-2020, with additional contributions from other programmes, but these were not sufficient to address the scale of the challenge[7]. The lack of sufficient investment and coordination at EU level was seen as a key barrier to building resilience and supporting the digital single market.

Stakeholder perceptions and consultations data

[4] EUR-Lex - 52017SC0500 - EN - EUR-Lex
[5] McAfee & Center for Strategic and International Studies, 'Net Losses: Estimating the Global Cost of Cybercrime', 2014.
[6] As per CSA 2017 IA; Source: White House, Factsheet Cybersecurity National Action Plan.
[7] CSA 2017 IA.

Stakeholder consultations for the 2017 IA included a call for evidence, targeted surveys, workshops and interviews with a wide range of actors, including public authorities, EU institutions, industry, academia, civil society and individual citizens. The main findings were as follows:

- A large majority of respondents positively assessed ENISA's performance for 2013-2016 and a significant proportion considered ENISA to be achieving its objectives.
- Many appreciated ENISA's products and services as coming from an EU-level body and valued their quality.
- A large majority considered current EU instruments and mechanisms insufficient or only partially adequate to address cybersecurity challenges and almost all saw a need for an EU body to respond, with most identifying ENISA as the right organisation.
- A significant proportion of respondents to the ENISA consultation saw a role for ENISA in establishing a harmonised framework for ICT security certification.
- Many respondents to the 2016 consultation for the preparation of the EU cybersecurity contractual public-private partnership (cPPP)[8][9], which devoted a section to the topic of certification, did not know whether national certification schemes were mutually recognised, with only a minority saying 'Yes'[10].
- A substantial proportion thought existing certification schemes did not support the needs of Europe's industry, and many said it was not easy to demonstrate equivalence between standards, certification schemes and labels.
- Many respondents experienced barriers to market access and export due to fragmentation and a significant number of SME respondents identified the cost of certification as a problem.

Stakeholders consistently identified the most urgent gaps to be in cooperation across Member States, capacity to prevent and resolve large-scale attacks and the need for harmonised standards and certification. The consultations also revealed that while ENISA was valued for its expertise and its role in community building, there was a strong call for a more permanent, better-resourced agency with a clearer mandate and greater operational capacity.

In summary, the baseline scenario in 2017 was a small, under-resourced ENISA with a fixed-term mandate, a fragmented and costly certification landscape, significant economic losses due to cybercrime and widespread stakeholder recognition of the need for greater EU-level coordination, harmonisation and investment. The lack of mutual recognition of certification schemes, high costs and long processes and insufficient EU-level operational capacity were seen as major barriers to a secure and competitive digital single market. These baseline conditions provide the foundation for assessing the effectiveness and

[8] Contractual Public-Private Partnership on cybersecurity, signed by the European Commission and the European Cyber Security Organisation (ECSO) on 5 July 2016.

[9] Commission Staff Working Document: Report on the public consultation and other consultation activities of the European Commission for the preparation of the EU Cybersecurity contractual Public-Private Partnership and Accompanying Measures, accompanying the document Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation, SWD(2016) 215 final.

[10] In this 2016 public consultation, a section was devoted to the topic of ICT security certification. 240 stakeholders from national public administrations, large businesses, SMEs, microbusinesses and research bodies responded to the section on certification.

impact of the CSA and the reformed ENISA. The evidence presented here is drawn directly from the 2017 CSA IA, including its executive summary, problem definition, baseline scenario, economic analysis and stakeholder consultation sections.

3. HOW HAS THE SITUATION EVOLVED OVER THE EVALUATION PERIOD?

This chapter reviews how the EU's cybersecurity landscape has evolved over the evaluation period, highlighting the transformative impact of major legislative acts such as the Cybersecurity Act, NIS2 Directive, Cyber Resilience Act and Cyber Solidarity Act (both under development at the time of the evaluation). These laws, together with sector-specific regulations, have reshaped the mandates and activities of ENISA and the ECCF. The chapter outlines how new threats, rapid digitalisation and geopolitical tensions have driven regulatory and operational changes, setting the context for assessing the effectiveness, coherence and added value of the EU's action on cybersecurity.

Current state of play

Since the adoption of the CSA, the EU's cybersecurity environment has undergone profound changes. The world has seen a dramatic escalation in cyber threats, with attacks becoming more frequent, sophisticated and impactful. Geopolitical tensions, such as Russia's war of aggression against Ukraine, have brought cyber operations to the forefront of hybrid warfare. At the same time, the COVID-19 pandemic accelerated digitalisation, exposing new vulnerabilities as remote work and digital services expanded rapidly. These developments have fundamentally altered the risk landscape and prompted the EU to significantly strengthen its legal and policy framework for cybersecurity.

Expansion of the EU cybersecurity legal and policy framework

In response to these evolving challenges, the EU adopted new legislative and policy instruments (of which some were under development during the evaluation period), building on the foundation laid by the CSA, and which have been central to the EU's cybersecurity strategy:

- **NIS2 Directive (Directive (EU) 2022/2555):** This Directive makes a broader range of entities subject to cybersecurity requirements, strengthens risk management and incident reporting obligations and develops cooperation among Member States.
- **Cyber Resilience Act (CRA, Regulation (EU) 2024/2487**, under development during the evaluation period**):** The CRA introduces horizontal cybersecurity requirements for products with digital elements, aiming to ensure that hardware and software placed on the EU market are secure by design and by default considering their lifecycle.
- **Cyber Solidarity Act (CSoA, Regulation (EU) 2025/38,** under development during the evaluation period**):** The CSoA focuses on building Union capacities for detection, preparedness and response to significant and large-scale cyber incidents, including the establishment of the EU Cybersecurity Reserve.
- **Digital Operational Resilience Act (DORA, Regulation (EU) 2022/2554):** DORA sets out comprehensive requirements for the financial sector to ensure operational resilience against ICT-related incidents.
- **Network Code on Cybersecurity for Electricity (NCCS, Delegated Regulation (EU) 2024/1366**, under development during the evaluation period**):** The NCCS introduces sector-specific cybersecurity rules for the electricity sector, particularly for cross-border flows.

- **EU Regulation on Information Security (PART-IS, Regulation (EU) 2023/203):** PART-IS establishes information security requirements for the air transport sector.
- **5G Cybersecurity Toolbox (Commission Recommendation (EU) 2019/534):** This provides guidance for securing 5G networks across the EU by recommending strategic and technical measures.
- **Cybersecurity Skills Academy (COM(2023) 207 final):** This initiative addresses the growing gap in cybersecurity skills by promoting training and capacity building.
- **EU Action Plan on the Cybersecurity of Hospitals and Healthcare Providers (COM(2025) 10 final):** This plan aims to strengthen the resilience of the healthcare sector.

Together with the CSA, these legal and policy instruments form a comprehensive and multi-layered framework that addresses both horizontal and sector-specific cybersecurity challenges. They reflect the EU's recognition that cybersecurity is not only a technical issue but also a matter of economic security, public safety and strategic autonomy.

Implementation and operational developments

The implementation of the new legal framework has required significant adaptation by Member States, EU institutions and businesses. ENISA's mandate has expanded accordingly. ENISA now supports Member States in developing and updating national cybersecurity strategies, implementing new legal requirements and building operational capacity. By virtue of other legislation proposed at the time of evaluation and subsequently through the contribution agreements, ENISA has also been tasked with managing the European Vulnerability Database and supporting the EU Cybersecurity Reserve.

The ECCF, established by the CSA, has continued to evolve. ENISA has coordinated the development of candidate certification schemes, such as the EU Common Criteria (EUCC) and the forthcoming European Cloud Certification Scheme (EUCS). However, the process has been slower than anticipated, with the first scheme taking nearly five years from initiation to adoption. The reasons for the delays include the complexity of technical, legal and political negotiations, as well as the need for consensus among a wide range of stakeholders.

Monitoring arrangements have included regular reporting, stakeholder consultations and the use of indicators such as the number of training courses delivered, publications produced, and stakeholder engagement events held. ENISA's outputs have increased in both volume and scope, reflecting the growing demands on it.

Current situation and key developments

The cybersecurity threat landscape has become more complex and interconnected. Ransomware attacks, supply chain compromises and hybrid threats are now commonplace, affecting critical infrastructure, public services and businesses of all sizes. The average cost of a major cyber incident has risen sharply, with global estimates of overall cost exceeding EUR 5.5 trillion in 2020[11] and projected to reach EUR 9 trillion by 2025.

ENISA has responded by scaling up its activities, delivering a growing number of publications, technical guidelines and capacity-building events. ENISA has played a

[11] JOIN(2020) 18 final.

central role in supporting the implementation of new legislation, advising on incident response and facilitating information sharing among Member States. The ECCF has begun to deliver candidate certification schemes (with one scheme adopted), but the pace has been slower than originally envisaged and fragmentation persists due to differences in national approaches and resource allocation.

Delays, challenges and external factors

The implementation of the new legislative framework has not been without challenges. Delays in the adoption of certification schemes have limited the harmonisation of cybersecurity assurance across the EU. Both ENISA and national authorities are affected by resource constraints, including the shortage of skilled cybersecurity professionals. The regulatory landscape is complex, with overlapping horizontal and sector-specific requirements. This has created compliance challenges for businesses operating across multiple sectors.

External factors, such as the acceleration of digital transformation, the emergence of disruptive technologies like AI and quantum computing and intensifying geopolitical tensions, have all impacted the implementation of the EU's cybersecurity framework. Hybrid attacks, in which cyber operations are combined with other forms of aggression, have become a defining feature of the threat landscape.

Monitoring, indicators and further information

Throughout the evaluation period, ENISA's mandate and the ECCF have been monitored using a range of quantitative and qualitative indicators. These include the number of certification schemes adopted, the volume and reach of ENISA's outputs, the level of stakeholder engagement and feedback from stakeholder consultations. Further details and data can be found in the annexes to the evaluation report.

In summary, the evolution of the EU's cybersecurity landscape over the evaluation period has been shaped by a series of ambitious and far-reaching legislative initiatives. These new laws have been instrumental in driving change, expanding the regulatory framework and strengthening the capacity of Member States, EU institutions and businesses to address increasingly complex and dynamic cyber threats. Their implementation has also revealed important challenges, including delays, resource constraints and the ongoing need for harmonisation. The rapidly changing cyber threat landscape, technological advances and geopolitical developments increase the critical importance of these legislative measures and the need for continued adaptation and coordination at European level. This is the background to the subsequent analysis of the effectiveness, efficiency and added value of the CSA, ENISA's mandate and the ECCF.

4. EVALUATION FINDINGS (ANALYTICAL PART)

This chapter presents an analytical assessment of the CSA, ENISA's mandate and the ECCF, drawing on the study to support the evaluation of ENISA and the ECCF from 2024[12]. This chapter summarises the findings around the five evaluation criteria: effectiveness, efficiency, coherence, EU added value and relevance. Drawing on qualitative and quantitative evidence, including stakeholder surveys, interviews and performance data, this chapter compares the expected outcomes of the action with the actual situation observed during the evaluation period. The analysis provides an evidence-based assessment on the extent to which the action achieved its objectives, the difference it made for various stakeholders and its ongoing suitability in the face of evolving cybersecurity challenges and policy needs. References to supporting data and further details are provided throughout, with additional evidence available in the annexes.

4.1. To what extent was the intervention successful and why?

Effectiveness

ENISA

ENISA has fulfilled its mandate by delivering nearly all planned outputs. During challenging times, such as the COVID-19 pandemic and Russian war of aggression on Ukraine, ENISA demonstrated flexibility and was evaluated positively by stakeholders. ENISA's effectiveness stems from a robust governance structure and a matrix-based organisational model that facilitates task delivery and cooperation. However, while stakeholders valued ENISA's capacity-building efforts, there were occasionally delays due to ongoing resource constraints and rigid strategic plans. In particular, ENISA planned 219 outputs between 2017 and 2022 and delivered 203, often exceeding initial targets per output due to a higher-than-expected number of stakeholders engaged in its activities. Eight outputs were delivered to some extent and in three cases, outputs were not delivered or only partially achieved, due particularly to the COVID-19 pandemic. The results of five outputs were not reported entirely. ENISA's support for policy implementation was generally well received, with 93% of stakeholders expressing satisfaction with ENISA's added value in this area in 2022. ENISA contributed to national and EU policies and legislative initiatives, supported the implementation of the NIS Directive and played a key role in the development of the ECCF. In 2021, ENISA made 193 relevant contributions to EU and national policies and legislative initiatives, which increased to 314 in 2022. However, over 80% of these contributions were through organising workshops and conferences. In 2022, ENISA's reports, analyses and studies were referred to 65 times at EU and national levels. Between 2017 and 2023, ENISA produced and issued a total of 286 publications. These covered a wide range of topics, with the most frequent being cybersecurity policy (72 publications), cyber threats (48), critical infrastructure (38), incident reporting (24) and emerging technologies (21).

Among key outputs, ENISA's studies, such as the 2020 report on NIS investments[13], highlighted the challenges faced by organisations in implementing the NIS Directive, such as unclear expectations and limited support from national authorities. Moreover, the

[12] PPMI, Intellera Consulting and PwC (2024): Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report.

[13] NIS Investments Report 2020, https://www.enisa.europa.eu/publications/nis-investments

Agency's support to the NIS Cooperation Group Workstream on Digital infrastructure and service providers was crucial in analysing the security aspects of the digital infrastructure sector, which then fed into the NIS2 proposal to extend the scope of the sector. This analysis also assisted Member States in the development of guidelines by highlighting priorities and best practices within the industry.[14]

In 2023, ENISA's efforts in the implementation of the directive included the provision of technical advice to the Commission on the implementation of NIS2 security measures and the drafting of guidelines for national coordinated vulnerability disclosure policies.[15] The Agency supported the implementation of NIS2 by responding to 12 individual requests from Member States for advice on the transposition of the Directive into national legislation and by organising risk management training for national authorities to help build knowledge and expertise.

However, stakeholders also noted that ENISA's reports could be more concise, practical and better tailored to their needs, with improved visualisation and summaries. The lack of a more effective communication system and the complex structure of ENISA's website further complicated stakeholder interaction with ENISA's outputs. Some stakeholders called for more transparent processes, better tailored content and more detailed and pragmatic guidance, especially for sector-specific needs.

While ENISA has achieved many of its objectives, there is a clear opportunity for ENISA to enhance its efficiency through improved prioritisation, clear focus and more strategic resource allocation. ENISA's efficiency has been occasionally hampered by external factors and a need for more streamlined internal governance. Internally, ENISA has developed innovative solutions, such as a matrix-based organisational model, to coordinate between operational and administrative functions more effectively. However, ENISA's staff occupancy rate fluctuated between 74% and 90% from 2017 to 2023 and recruitment and retention of senior cybersecurity experts remained a persistent challenge. This impacted deliverables, with some outputs that were not delivered or only partially achieved.

There is also room to improve task prioritisation. By reassessing its operational focus, ENISA can leverage existing frameworks and stakeholder feedback to improve task delivery even further. This approach is particularly crucial for addressing emergent priorities without compromising on existing commitments. ENISA's ongoing commitment to stakeholder engagement and consultation has been a strength, yet its operational capacity shows insufficient resources. More dynamic reallocation of tasks and resources could help towards timely fulfilment of new requests and enhance ENISA's ability to respond to cybersecurity challenges to a certain extent.

ENISA's aim of maintaining and bolstering its reputation in the cybersecurity community could be further realised by ensuring that tasks are aligned not only with strategic goals but also with operational capacity. To this end, ENISA's mandate would need to be revised, supported by a continual process of resource evaluation and strategic reprioritisation. This structured approach will assist ENISA in navigating its evolving role within the EU cybersecurity framework more effectively, ultimately increasing its impact and sustaining its status as a flagship institution for cybersecurity initiatives. Such prioritisation should be facilitated through collaborative efforts between ENISA, Member

[14] ENISA, Annual Activity Report, 2020.
[15] ENISA, Annual Activity Report, 2023.

States, and EU policymakers to ensure alignment with strategic objectives and operational capacity.

ECCF

The ECCF was envisioned as a pillar for improving cybersecurity assurance across the EU internal market, aiming to harmonise the certification of ICT products, services, and processes. It sought to tackle persistent issues such as market fragmentation, the need for enhanced transparency, and raise public trust in digital solutions. Its structured governance model involving entities like ENISA and the European Cybersecurity Certification Group (ECCG), gathering National Cybersecurity Certification Authorities (NCCAs), has indeed laid a foundation for increased coordination among stakeholders, including Member States and private entities. However, the practical realisation of these goals has been met with numerous challenges that have restricted the ECCF's effectiveness. A significant shortcoming of the current ECCF is its inability to effectively address the fragmentation of certification schemes across the EU, mainly due to procedural limitations. This fragmentation has persisted even though the framework is intended to harmonise certification processes, leading to inconsistencies and inefficiencies in cybersecurity assurance. This can be observed in the substantial delay in operationalising the first certification scheme, the EUCC, which took 55 months from initiation to adoption. This delay points to inefficiencies, predominantly influenced by the complex and multifaceted approval procedures. Moreover, there is a certain lack of clarity about responsibilities and accountability among stakeholders. This has made achieving the framework objectives even more complex. External factors further complicated the ECCF's aims.

The evolving geopolitical landscape, characterised by increasing cyber threats and political tensions around data sovereignty and digital control, required adaptive measures that the ECCF struggled to implement swiftly. These external pressures resulted in delayed scheme adoptions, as seen with the EUCS, where discussions stalled over non-technical debates like data localisation requirements.

Despite these hurdles, there have been positive outcomes–particularly in raising awareness across Member States about the importance and intricacies of cybersecurity certification. The COVID-19 pandemic, while causing operational delays, also made the necessity for resilient digital infrastructure even clearer, thrusting cybersecurity into the policy spotlight. Additionally, the analysis identified key lessons, noting the uneven resource allocation across stakeholders, which hinders the uniform development and deployment of certification schemes. National authorities acknowledged the support of the ECCF in building national cybersecurity certification capabilities but noted significant resource imbalances between Member States. For example, the number of FTEs was seven times higher in one Member State compared to another one for similar activities of issuing certificates. Also, ENISA stated that due to the difficulty of retaining staff and the competitive job market for cybersecurity professionals, it could not maintain its full staff level (including for certification) at times. Addressing these disparities is vital for future efficiency and effectiveness, particularly through retaining expert staff within ENISA and fostering constant dialogue among all parties involved.

Despite these challenges, the ECCF did improve harmonisation among Member States and established better cooperation opportunities, particularly through the creation of stakeholder cooperation forums such as the ECCG. Most participants during the interview process agreed that the ECCF established better cooperation opportunities for Member States and the majority of Member State representatives interviewed agreed that the ECCF improved harmonisation among Member States. Statements gathered during interviews

underlined the importance of the ECCF support to Member States when Member States developed their capabilities. For instance, one national authority reported how it benefited from cooperation among Member States by acquiring knowledge in areas where it lacked expertise, while others stressed the pedagogical value that cooperation among ECCG members can have. However, national experts stressed that the ECCF strengths remained 'potential' due to the lack of scheme implementation so far.

Efficiency

ENISA

During the evaluation period, which spanned from 2017 to 2023, ENISA demonstrated efficient operations under its existing governance structure. The matrix-based organisational framework helped ENISA prioritise tasks, optimised resource alignment, and fostered cooperation between various units. This approach, coupled with a balanced mix of operational and administrative staff, helped facilitate the execution of its mandated duties. Despite this, the evaluation highlighted several key areas where ENISA has room to improve its efficiency. Interviews with ENISA's staff, stakeholder surveys and internal documentation indicated that ENISA struggled to keep pace with increasing demands and fill specialised positions, exacerbated by a global shortage of IT and cybersecurity specialists. This has led to delays, reprioritisation of tasks, and periods of high stress and workload. Stakeholders gave a positive assessment of ENISA's performance during periods of high workload, with 63% of respondents stating that ENISA was successful or very successful in delivering its outputs. However, resource constraints, operational inefficiencies and challenges stemming from the political and regulatory environment were identified as the main obstacles to ENISA's performance during periods of high workload. In 2022, 64% of respondents experienced stress due to high workload and 43% due to high administrative burden. Only 32% gave a positive assessment of stress management.

Nevertheless, certain adjustments could alleviate these challenges. The recent strategic decisions to reallocate human resources demonstrate a capacity that can address priority shifts to a certain extent. For instance, the reallocation of approximately 10.5 FTEs planned in 2022 to accommodate the Cybersecurity Support Action suggests that ENISA is able to optimise current resources when necessary even though, on that occasion, the FTEs needed for the implementation of the Support Action were in fact obtained partially through procurement and partially through contract management staff.

Budget management also presents opportunities for improvement. Despite significant budget growth from 2017 to 2023, resource constraints persisted. ENISA's budget grew unevenly, with notable increases in 2019 (over 46%), 2020 (30.5%) and 2022 (72.4% compared to 2021, due to the Cybersecurity Support Action). ENISA was less able to balance approved and committed appropriations between 2019 and 2022 due to delays in actions like the Cybersecurity Support Action. By reversing this trend and making efforts to manage administrative expenditure, including addressing procurement delays, internal efficiency could see certain further enhancement.

ECCF

The efficiency of the ECCF has been subject to scrutiny, given the extended timelines for the adoption of cybersecurity certification schemes and the myriad of complexities involved. Despite its strategic aim of streamlining the certification process across the EU, the ECCF's efficiency was notably hampered by drawn-out discussions and preparation phases that culminated in significant delays; the first scheme EUCC was only adopted in

early 2024, nearly five years post-implementation. These protracted timelines can be attributed to multifaceted challenges encompassing both political and technical dimensions.

Given the recent adoption of the EUCC scheme, it is premature to identify costs borne or benefits experienced by stakeholders for compliance with ECCF requirements. Survey respondents indicated some costs and benefits related to preparatory activities. Benefits include enhanced cooperation, knowledge exchange, growing awareness and contribution to standard development. Costs include dissemination and awareness support, pilot implementations, legal consultations for aligning national requirements, setting up of web portals and reporting mechanisms and CAB accreditation. Stakeholders involved in preparing schemes bore costs related to scheme development, publication and communication efforts, including investment in staff allocation and upskilling.

Content and process-related issues had the greatest impact on the efficiency of the ECCF. Content issues included political factors and the technical complexity of schemes, which varied for each scheme depending on the stakeholders involved and products/services to be certified.

More generally, political challenges, including the politicisation of discussions around certification requirements, have hindered progress by creating an environment where transparency and communication suffered. For instance, the EUCS was impacted significantly by debates around data sovereignty requirements, attracting political pressure from non-EU countries and industry outside the EU, leading to shifts from technical to political discourse within the ECCG. Moreover, the scheme was impacted by a shift in EU policy priorities due to the concurrent proposal of the CRA in September 2022.

Technical complexities further contributed to inefficiencies, notably the difficulty in translating draft schemes into legal acts, given the diverse and demanding nature of the products/services slated for certification, such as 5G and cloud computing. The wide-ranging requests and lack of established standards in certain areas added layers of difficulty to the preparation and adoption processes, necessitating a multitude of stakeholders and phases to ensure alignment with existing policies and practices. Stakeholders confirmed the difficulty of converting an existing international certification mechanism (SOG-IS) into EU law and highlighted the need for more structured engagement in the framework through clear processes and realistic timelines. Despite these inefficiencies, several positive elements arose within the framework. The formation of dedicated groups and forums, including the ECCG, the Ad Hoc Working Group (AHWG) dedicated to specific schemes and the Stakeholder Cybersecurity Certification Group (SCCG), facilitated necessary stakeholder involvement. Nonetheless, there remains substantial room for improvement in ensuring these structures function optimally as, for example perceived lack of involvement of the SCCG members in the ECCF. Refinement of internal governance is crucial to increase the active participation and strategic input of stakeholders.

Coherence

ENISA

In assessing ENISA's coherence, the evaluation highlights both strengths and areas for improvement. ENISA's commitment to fostering cybersecurity cooperation at the EU level

is apparent, particularly through its facilitation and direct engagement with stakeholders. ENISA supported EU networks such as the CSIRTs network and EU-CyCLONe and facilitated the exchange of best practices through the NIS Cooperation Group and organised exercises such as CyberEurope. Despite some overlaps with national cybersecurity authorities and CERT-EU, ENISA's efforts were largely complementary, with effective exploitation of synergies and knowledge sharing. Survey data indicated that 74% of stakeholders overall agreed that ENISA sufficiently exploited synergies in expertise and knowledge sharing with other actors, with representatives of private bodies slightly less satisfied (65%).

This dual approach has enabled ENISA to significantly contribute to the cyber domain, aligning with recent legislative frameworks. However, while ENISA's role as a facilitator and coordinator is positive, several areas require improvement to enhance coherence. The evaluation identified the need to improve synergies between the responsibilities and actions of ENISA and other EU bodies such as the European Cybersecurity Competence Centre (ECCC), as well as national cybersecurity authorities. Although these roles are often complementary, opportunities exist to further streamline operations and improve organisational efficiency. By formalising cooperation arrangements with other entities, such as EMSA and the JRC, ENISA could better leverage synergies and ensure a unified approach to cybersecurity initiatives. Internal communication and resource management within ENISA should also be refined. ENISA's interaction with private stakeholders and international partners must be more predictable and transparent to maintain confidence and foster collaborative efforts. In this context, private entities, while considering ENISA's contribution beneficial, suggested that ENISA's stakeholder engagement activities could be improved, particularly in relation to collaboration with industry representatives and non-EU countries.

In alignment with the CRA and NIS2 Directive, a clear delineation of ENISA's tasks supporting policy implementation could increase efficiency and ensure consistency across regulatory measures. This clarity would also improve ENISA's ability to respond to sectoral regulatory requirements.

In summary, while ENISA has demonstrated a solid foundation in promoting cybersecurity coherence in the EU, there is potential for it to reprioritise its efforts. This approach will help it to efficiently fulfil its mandate and adapt to the evolving cybersecurity landscape. By addressing current inefficiencies and enhancing inter-agency coordination, ENISA can effectively maintain its crucial role within the EU's cybersecurity framework.

ECCF

The ECCF's coherence is affected by the lack of clear accountability mechanisms, which has led to difficulties in aligning its objectives with other legislative measures. This misalignment risks creating overlaps and inefficiencies in the cybersecurity landscape. To ensure a unified approach to cybersecurity, the ECCF needs to be completely coherent with other EU legislative instruments, including the NIS2 Directive and the CRA. In theory, the ECCF is aligned with these legislative measures, designed to address various facets of cybersecurity within the EU landscape, yet real-world integration remains complex and requires diligent oversight. The forthcoming implementation of the EUCC scheme poses a significant test for this coherence: if the scheme is successfully deployed, it will demonstrate the ECCF's ability to harmonise and effectively leverage additional legislative efforts. Stakeholders have emphasised the need for careful coordination between the ECCF and emerging regulatory acts to prevent potential overlaps which could undermine efficiency and dilute intended effects across sectors. Specifically, concerns

arise regarding the interface between the ECCF and the CRA, as both initiatives aim to raise cybersecurity standards but risk redundancy if not fully synchronised. On the sectoral side, coherence must extend to accommodate continuing advancements in technologies, ensuring that cybersecurity initiatives are appropriately nuanced to address critical infrastructure needs.

Survey data showed that 83% of stakeholders found the ECCF to be coherent with other EU instruments, with 55% rating it as fairly coherent, 23% as very coherent and 5% as perfectly coherent. However, concerns remain about potential overlaps, particularly with the CRA, which could result in duplication of efforts and inconsistent requirements. More than half of respondents identified overlaps between the ECCF and other EU initiatives. Member States stressed the importance of ensuring coherent implementation of the CSA and CRA and highlighted the need to establish communication channels with international organisations to leverage existing European or international standards and prevent inconsistencies between standards developed at the EU and international levels.

4.2. How did the EU intervention make a difference and to whom?

EU added value

ENISA

ENISA has significantly contributed to enhancing the EU's cybersecurity ecosystem, yet there are opportunities for improvement that could amplify its impact. Serving as a centralised hub, ENISA has facilitated vital cooperation across the EU. It has complemented national efforts, especially in Member States with less developed cybersecurity infrastructures, and aligned cybersecurity practices and policies. Around two thirds of surveyed stakeholders considered that without ENISA, the collection and dissemination of relevant cybersecurity information, the generation of new knowledge, insights and evidence on cybersecurity issues and supporting the implementation of EU cybersecurity policies at the national level would be hard to achieve. Three quarters of respondents believed that without ENISA there would be little effect on improving Member States' cybersecurity capacities, as well as raising awareness of cybersecurity issues. As a decentralised EU Agency, ENISA's specialised mandate has allowed it to consolidate cybersecurity expertise and engage effectively with Member States, playing a pivotal role in shaping Europe's cybersecurity landscape. In this context, ENISA's main focus on Member States is essential, given its role in providing insights into emerging threats and recommending tools and strategies for addressing them.

Moreover, ENISA plays a critical part in promoting cybersecurity certification and supporting standardisation activities, which helps reduce market fragmentation and fosters robust cybersecurity practices across the EU. Although no other similar bodies with ENISA's expertise and organisational agility exist, its current primary focus on national authorities has attracted criticism from private sector stakeholders. Feedback from large industry players indicates that more could be done to tailor insights to the private sector's specific challenges. Companies reported that they often relied on ISO/IEC standards rather than ENISA schemes. Some organisations valued ENISA's technical guidelines, tools and reports, although they claimed some of them were redundant with existing standards. Though the primary focus on national authorities is crucial, ENISA could address these concerns by strategically improving engagement with stakeholders and collaboration with the industry. Additionally, ENISA's mandate could benefit from strategically reassessing its priorities to adeptly adapt to evolving cybersecurity challenges. This would allow

ENISA to maintain its valuable contributions to the EU, while effectively addressing the expanding needs of its varied stakeholders.

Key achievements and challenges

ENISA is widely recognised within the EU's cybersecurity community for its robust reputation, quality publications and significant role in fostering cooperation among Member States and other cybersecurity entities. ENISA's work on harmonising cybersecurity requirements is crucial in establishing a consistent level of protection across Member States, contributing directly to capacity building, especially for smaller Member States. This harmonisation not only ensures a secure digital environment across the EU but also elevates cybersecurity preparedness across its stakeholders.

However, the evaluation identified several challenges faced by ENISA. ENISA shows limited agility in responding to evolving cybersecurity threats which may lead to potential delays in its activities. To mitigate the problems of limited resources, the stakeholders[2] emphasised the need for improved recruitment processes and workload management strategies. Expanding ENISA's mandate to extend its operational role could address these concerns, allowing it to leverage technological advancements and improve cybersecurity frameworks. This restructuring would enable ENISA to proactively tackle dynamic threats, increasing its impact through joint training initiatives and making a contribution to policy-making processes.

Finally, ENISA's stakeholder consultation and management systems are deemed effective in facilitating management of stakeholder needs and expectations. However, a stronger, more transparent relationship with Member States is necessary to develop cooperation and information sharing. Future priorities include updating internal frameworks to better manage growing responsibilities and diverse challenges, ensuring that ENISA can fully implement its mandated tasks given its staff size.

ECCF

Despite its potential, the ECCF has struggled to deliver added value in fostering a unified and effective cybersecurity environment across the EU. The ECCF sought to significantly enhance the EU's cybersecurity landscape by introducing an unprecedented development procedure and governance structure for certification processes. At its core, the ECCF represented a critical advancement in the EU's ability to create a harmonised approach to the certification of ICT products, services, and processes. The inherent EU added value of this framework lies in its potential to bridge disparate national approaches, fostering an internal market with consistent, reliable, and recognised cybersecurity standards across Member States. However, the protracted timelines and fragmented implementation have impeded the ECCF's ability to fully capitalise on its envisioned value. Specifically, the delay in actionable schemes, evidenced by the late adoption of initiatives like the EUCC, curtailed immediate impacts, leaving its theoretical potential largely unfulfilled.

The EUCC was adopted in January 2024, 4.5 years after the Commission request was introduced. Based on interviews with Commission, Member States and ENISA, this long timeframe of development and adoption can be attributed to a mix of factors. First, delay was caused by the lack of experience in developing and adopting schemes. Stakeholders confirmed the difficulty of translating the ENISA candidate scheme endorsed by the ECCG into an EU legal text both for the Commission draft implementing act and during the comitology procedure. Stakeholders also confirmed the difficulty of converting an existing

intergovernmental certification mechanism (Senior Officials Group Information Systems Security – SOG-IS) into EU law that raised challenges related both to technical complexities and harmonisation with the repeal of national schemes. Moreover, the scheme was impacted by a shift in EU policy priorities due to the concurrent proposal of the CRA in September 2022, as well as by staff turnover and shortage from the Commission side.

The request for EUCS was introduced in November 2019 building on previous stakeholder-driven efforts that started in 2017. According to surveyed stakeholders, the adoption of the EUCS scheme was primarily impeded by issues related to its content and largely due to the politicisation of the debate, which contributed to divide Member States positions within the ECCG. As emerged from the call for evidence and confirmed by interviews with all relevant stakeholder categories (i.e. national authorities, EU institutions and agencies and industry), the discussions surrounding sovereignty concerns resulted in polarized discussion around the draft scheme in the institutional and public spheres. Furthermore, the situation around the EUCS triggered debates related to the scope of the ECCF as well as criticism from stakeholders regarding insufficient involvement in scheme development processes, due to a lack of transparency.

Disparities in systemic implementation, compounded by varying degrees of readiness and resource availability among Member States, further dilute the framework's comprehensive influence. Nevertheless, the ECCF has invigorated cooperative dynamics across the EU. By establishing groups such as the ECCG, it has institutionalised coordination efforts, enabling broader engagement across different governance levels. This collaborative infrastructure encourages information sharing and joint strategies, promoting a unified cybersecurity stance against evolving threats. While the direct influence of the ECCF is limited, stakeholders broadly agreed that the framework brings EU added value compared to what could have been achieved by Member States alone. 92% of stakeholders believed that Member States alone could not have achieved more streamlined and cost-effective certification processes, specifically in terms of uptake of certification, cost-effective processes, cyber-awareness, trust in the EU single market and cybersecurity by default and design. Most stakeholders recognise the added value of the ECCF in achieving a more secure, transparent and cohesive internal market for ICT products, services and processes. According to 88% of stakeholders, Member States alone might not be able (or able only in a limited way) to increase trust and awareness of citizens and businesses regarding the cybersecurity of ICT products, processes and services alone. This suggests the ECCF helps enhance trust.

For the ECCF to unlock its full EU added value, increased and concise stakeholder participation is critical. Fostering an inclusive environment where industry partners, national authorities, and EU bodies actively contribute to and guide the certification process will ensure widespread acceptance and effectiveness of cybersecurity standards.

Key achievements and challenges

The ECCF serves as a critical tool for enhancing EU-level collaboration between ENISA, Member States, and industries. Therefore, it has considerable relevance in the dynamic cybersecurity environment. Its adaptability facilitates scheme development through ad hoc working groups and aligns with EU legislative frameworks like NIS2. This potential, while significant, remains largely untapped due to limited implementation of actual schemes.

The ECCF is pivotal in addressing emerging cybersecurity threats and fostering compliance, particularly in leveraging new technologies such as artificial intelligence.

Stakeholders acknowledge its role in strengthening cooperation among Member States and improving cybersecurity preparedness. Its value in fostering internal market exchanges, by replacing national certification schemes with EU-wide ones, is also recognised.

However, the ECCF is hampered by significant weaknesses. Lengthy processes for adopting schemes hinder its effectiveness, a challenge exacerbated by technical complexities and political pressures from industry lobbying. These delays undermine trust and prevent the swift adoption of standards. Opportunities exist for the ECCF to enhance EU cybersecurity frameworks, yet threats like resource constraints and geopolitical tensions pose challenges. Shifts in policy priorities and potential legislative overlaps could make the framework less effective, risking market inconsistencies. Addressing these issues is vital for ensuring the ECCF's evolution from a promising concept into a fully operational mechanism, bolstering EU cybersecurity standardisation and certification.

4.3. Is the intervention still relevant?

Relevance

ENISA

ENISA's relevance within the cybersecurity domain is also due to its responsiveness to evolving stakeholder needs and its flexibility to adapt to the changing landscape. ENISA has consistently demonstrated its ability to review and realign its areas of action to address emerging developments, thereby maintaining its position as a vital component in the EU's cybersecurity framework. For example, in 2020, ENISA established the Ad hoc Working Group on Artificial Intelligence Cybersecurity to address the growing need to map the AI threat landscape and develop security measures. In 2021, it set up an interdisciplinary working group on emerging and future cybersecurity challenges, integrating foresight into cybersecurity practices and increasing awareness of future threats.

While stakeholder satisfaction with ENISA's efforts is generally positive, 44% of the surveyed stakeholders and 50% of industry representatives indicated their needs were met only 'somewhat', 'to a small extent', or 'not at all' by ENISA's services and outputs. There are dimensions where its relevance can be further enhanced. Despite its responsive nature, ENISA could still further improve support and increase visibility among diverse sectors and stakeholders, particularly for SMEs, which often struggle to adhere to cybersecurity requirements. A shift towards providing more direct tools and resources tailored to specific sectors but also providing insights in and tools to address emerging threats can increase ENISA's impact. ENISA's approach to stakeholder engagement was effective, utilising forums, committees and working groups to actively involve national experts in operations and publications. However, the complex decentralised structure within some Member States posed challenges that could be mitigated by better organisation and clearer coordination with national authorities. ENISA's ongoing initiatives, including the development of cybersecurity guidelines and capacity-building programmes, reflect its commitment to fostering cooperation and reinforcing the EU's collective cybersecurity posture. Stronger collaboration across industries and improved information access could address some limitations perceived by the industry sector.

What would really help ENISA to vastly improve would be re-evaluating priorities, streamlining processes, acquiring new appropriate resources and maximising existing resources efficiently, thereby reinforcing its foundational role in Europe's cybersecurity ecosystem. Through strategic alignment with the European cybersecurity strategy, ENISA's new priorities could create pathways towards contributions with greater impact.

For ENISA to improve its capacity to provide policy and technical support, it might need to provide more resources, be more selective with its engagements and refine its operational focus areas. In conclusion, while ENISA's relevance is clear, there is still room for improvement.

ECCF

The ECCF has emerged as a crucial response to the growing complexity and sophistication of cyber threats across the EU. It aspires to establish harmonised cybersecurity certification schemes that ensure trust and foster a secure digital market. Despite its promising premise, the framework's relevance is still considered more potential than practical, with certification schemes only recently entering the operational phase. The lack of tangible results so far is a sign that implementation is uneven and means the ECCF's current standing in the cybersecurity landscape is uncertain. The significance of the ECCF lies in its strategic role in raising cybersecurity standards and enabling mutual recognition of certifications across Member States, thereby reducing individual enterprise costs and strengthening the internal market. The ECCF seeks robust integration with other EU legal acts, aiming to streamline procedures and facilitate cross-border trade. Yet the protracted timeline for scheme deployment and the discrepancy in expertise and resources among Member States make it much harder for the ECCF to realise its full potential. These challenges hinder collaborative efforts and impede the standardisation process that is central to the ECCF's mission.

Despite these challenges, there are several factors ensuring the ECCF's relevance. One is that the surge in cyber threats intensifies the need for a united cybersecurity strategy that can adapt swiftly to changing scenarios, such as the increased relevance of certification in high-assurance areas like cloud services and 5G infrastructures. Public procurement mandates in these sectors reflect the growing demand for a unified and reliable certification framework that the ECCF can fulfil. Furthermore, the ECCF is linked to emerging legislative acts, notably the CRA and NIS2 Directive, which points to its value in addressing critical infrastructure needs and legal conformity across the EU. ENISA's proactive role and the establishment of NCCAs mark crucial milestones towards strengthening collaborative interactions and promoting certification adoption. However, there are considerable differences between larger and smaller Member States when it comes to resource allocation and expertise, meaning continued imbalances in participation and effectiveness that impact the development of a collective scheme.

In conclusion, the evaluation finds that EU action has delivered relevant benefits in strengthening the cybersecurity landscape across the EU. ENISA has established itself as a centre of expertise, a facilitator of cooperation and a key contributor to policy development and capacity building, particularly for Member States with less developed cybersecurity capabilities. The ECCF, while still in the early stages of implementation, has laid the groundwork for harmonised certification and increased trust in digital products and services. However, both ENISA and ECCF have faced significant challenges, including resource constraints, delays in scheme adoption and the complexity of aligning with a rapidly evolving legislative and technological environment. Despite these obstacles, they remain highly relevant and continue to provide clear EU added value, especially in fostering cross-border cooperation, supporting SMEs and addressing emerging threats. The findings highlight the need for ongoing adaptation, increased resources and enhanced stakeholder engagement to ensure that the EU's cybersecurity framework remains effective, efficient and fit for future challenges.

5. WHAT ARE THE CONCLUSIONS AND LESSONS LEARNED?

This chapter synthesises the main conclusions and lessons learned from the evaluation of EU action on cybersecurity, focusing on ENISA and the ECCF. It provides policy-relevant insights for future development while staying within the limits of a staff working document. The conclusions are based on a systematic screening of evidence from performance data, stakeholder consultations and targeted workshops, highlighting what has worked, what remains uncertain and where challenges persist. Lessons learned are presented as part of the narrative, with attention to regulatory simplification and burden reduction.

5.1. Conclusions

The evaluation of ENISA highlights its crucial role in working towards a cohesive cybersecurity landscape across the EU. Although ENISA has shown effectiveness in parts of its mandate and generating valuable outputs, there remains significant room for improvement in handling external disruptions and meeting stakeholder expectations consistently. As demands on ENISA continue to grow, it is important to reassess its mandate and resources to better align it with priorities, with continued emphasis on supporting Member States as they address cybersecurity threats and improve their national cybersecurity infrastructures. Making ENISA more effective would require refinement of its report production process, making reports more tailored to stakeholder needs as well as more user-friendly and accessible through visual aids and concise summaries. Strengthening communication channels is essential to ensure ENISA's activities and services are clearly visible to stakeholders, including industry players. A well-defined communication strategy will aid in fostering stronger connections and cooperation within existing cybersecurity networks such as ISACs.

ENISA can become more efficient through a more strategic focus on task prioritisation, enabling a more streamlined approach to managing workload pressures. To become more relevant to stakeholders, ENISA should continue to expand its central role in supporting Member States by strengthening its capacity to provide timely insights into emerging threats and strategic tools for addressing them. Moreover, as a number of stakeholders noted, ENISA could establish more structured and transparent methods of engaging with private entities, with an emphasis on supporting SMEs. Clarity should be sought regarding ENISA's role in policy implementation with other EU institutions, ensuring that collaboration with Member States is at the forefront of these efforts to reinforce the cohesion of the EU's unified cybersecurity strategy, which would also include strengthening cooperation with other EU agencies and seeking synergies with other cybersecurity bodies for joint actions to improve operational coherence across Europe.

Overall, maintaining ENISA's status as a specialised agency within the EU framework is important, as it ensures continued focus on cybersecurity priorities.

The ECCF has partially achieved its objectives. It has succeeded in improving cooperation and coordination among Member States, EU institutions and the private sector, notably through the creation of forums such as the ECCG and to a lesser extent, the SCCG. These structures have facilitated knowledge sharing and harmonisation, but delays in the adoption of certification schemes, most notably the EUCC, which took nearly five years to implement, have limited ECCF's impact on market fragmentation, trust and transparency. The lack of implemented schemes means that many of ECCF's strengths

remain 'potential' rather than realised and the benefits for businesses and citizens are yet to materialise.

The evaluation finds that the EU's role has been essential in bringing together diverse actors to work on shared solutions that would not have been possible at national level. ENISA's decentralised structure and the ECCF's harmonised approach have enabled economies of scale and safeguarded key EU interests in cybersecurity. Stakeholders consistently noted that, without EU involvement, coordination, expertise development and cross-border cooperation would be significantly weaker, leading to fragmented approaches and increased costs.

Unintended effects have also emerged. The politicisation of debates around certification schemes (e.g. cloud sovereignty requirements) has led to delays and decreased trust among stakeholders. Nevertheless, the overall impact of the action remains positive, with stakeholders recognising the need for continued adaptation and coordination.

In terms of regulatory simplification and burden reduction (REFIT), the evaluation highlights the importance of streamlining reporting requirements, improving communication channels and making ENISA's outputs more accessible and tailored to stakeholder needs. Stakeholders suggested that more concise, practical reports and greater use of visualisations would enhance effectiveness and reduce unnecessary complexity.

5.2. Lessons learned

The evaluation yields several lessons that are relevant for future policy development, while acknowledging that some findings remain preliminary and require ongoing monitoring.

First, ENISA's expanding mandate and the evolving cybersecurity landscape would benefit from a **flexible approach to resource allocation and prioritisation**. ENISA's effectiveness depends on its ability to match its growing responsibilities with adequate human and financial resources. Lessons from stakeholder consultations indicate that secondment of national officials, partnerships with academic institutions and targeted recruitment programmes could go some way to addressing resource gaps and improving capacity.

Second, the **quality of stakeholder engagement** is a critical determinant of success. ENISA's effectiveness, efficiency and relevance are closely linked to its relationships with Member States, EU institutions and industry. The evaluation suggests that ENISA could further develop its cooperation strategies, including clearer communication campaigns, more structured engagement with industry (especially SMEs) and improved feedback mechanisms.

Third, the ECCF's experience highlights the importance of having **clear roles and responsibilities in scheme implementation and maintenance**. Despite ENISA's pivotal role in fostering cooperation and operational cohesiveness among Member States and other stakeholders, constraints on the efficiency and effectiveness of the ECCF have been evident, mainly due to the complexities of scheme adoption processes. These issues highlight the necessity of a substantial revision in governance structures to improve operational clarity and accountability at all levels. The evaluation also points to the importance for more granular scheme requests, early preparatory analysis and regular updates to work programmes to align expectations and smoothen adoption processes.

Fourth, developing **streamlined decision-making processes** within the ECCF which clarify roles and responsibilities will promote transparency and efficiency, particularly in collaborative efforts among Member States, the Commission, and ENISA. This will foster accountability and reduce inefficiencies.

Fifth, a commitment to **setting and adhering to realistic timelines** for the development and implementation of certification schemes is essential. This involves supporting detailed technical analysis and bolstering preparatory efforts to effectively anticipate and mitigate political influences.

Sixth, actively investing in the **training and retention of skilled personnel** within ENISA is crucial to ensuring continuity and expertise when navigating complex cybersecurity challenges. Long-term workforce stability will be vital to maintaining the ECCF's operational efficacy.

Seventh, industry and consumer **awareness about the ECCF could be increased** through targeted campaigns and strategic involvement, emphasising the value of certified products and services. A proactive approach to garnering stakeholder support is critical to boosting demand and trust in ECCF initiatives.

Eighth, the relevance and **added value of these efforts remain 'potential'** until schemes are fully implemented and maintained. Promoting uptake among industry, raising awareness among consumers and linking scheme planning to threat monitoring and legislative developments are essential for realising the full benefits of the ECCF.

Finally, the evaluation identifies opportunities for **regulatory simplification and burden reduction**. Streamlining administrative processes, clarifying terminology and harmonising requirements across legislative acts can help reduce unnecessary complexity and improve efficiency. Stakeholders emphasised the value of voluntary approaches, clear guidance documents and coordinated implementation to avoid overlaps and ensure coherence.

Some findings, such as the long-term impact of new certification schemes and the effectiveness of market surveillance, are too preliminary to draw firm conclusions and warrant a 'wait and see' approach. Ongoing monitoring and stakeholder engagement will be necessary to assess whether these issues resolve themselves over time or require further intervention.

ANNEX I: PROCEDURAL INFORMATION

1. Lead DG, Decide Planning/CWP references

Lead DG: Directorate-General for Communications Networks Content and Technology (CNECT).

Decide: PLAN/2023/181

Evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework

2. Organisation and timing

14 July 2023 - 4 December 2024 – The call for evidence was launched on 14 July 2023 (see below) and the final study report was delivered on 4 December 2024 (see below).

3. Consultation of the RSB

N/A

4. Evidence, sources and quality

Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework according to Regulation (EU) 2019/881 – STUDY 2023/037, carried out for the European Commission by PwC EU Services EESV, Open Evidence S.L. and PPMI Group, UAB – Final report 4 December 2024

A call for evidence on the impact, effectiveness and efficiency of ENISA's mandate and of the provisions of the European Cybersecurity Certification Framework (ECCF) was conducted from 14 July 2023 to 16 September 2023. The call for evidence was intended to elicit feedback from relevant stakeholders involved in the cybersecurity domain, and, more specifically, from those involved in the EU certification process. Overall, 41 stakeholders contributed to the call for evidence, mostly from the private sector.

ANNEX II. METHODOLOGY AND ANALYTICAL MODELS USED

Provide a critical assessment of the work carried out by the external contractor which allows an understanding of why you agreed or disagreed with their conclusions.

This annex provides a detailed account of the methodology and analytical approaches used in the evaluation of ENISA and the ECCF, as documented in the 2024 ENISA and ECCF Evaluation Report. This annex explains the data collection process, sources and stakeholder consultation activities, as well as the analytical techniques and validation steps applied throughout the evaluation. It also addresses any changes from the original plan, known limitations and the measures taken to ensure the reliability and robustness of the findings. The information presented here is intended to ensure full transparency and to support the credibility of the conclusions of the evaluation.

1. Overview and process

The evaluation of ENISA and the ECCF was conducted through a comprehensive, multi-method approach designed to ensure transparency, robustness and stakeholder engagement at every stage. The study was carried out by an external contractor, with close involvement and oversight from the European Commission. All planned activities, including surveys, interviews, workshops and desk research, were completed as scheduled, with only minor adaptations to the original plan as set out in the evaluation roadmap. Where challenges arose, such as difficulties in engaging certain stakeholder groups, mitigating measures were implemented to ensure the integrity and completeness of the evidence base.

2. Data collection and sources

Desk research and administrative data

Administrative and monitoring data provided by ENISA and the Commission formed the cornerstone of the evaluation. These data were used to assess the efficiency of ENISA, triangulate stakeholder perspectives and provide a factual basis for answering the evaluation questions. Internal documents, including minutes, reports and audits, were systematically reviewed to complement and validate findings from other sources.

For the ECCF, the evaluation focused on legislative texts, notably the Cybersecurity Act and its amendments, as well as new legislative documents such as the NIS2 Directive, CRA and the Union Rolling Work Programme (URWP). The Commission's call for evidence on the ECCF was also analysed, with particular attention to feedback from SCCG members.

Document and literature review

The literature review drew primarily on official documents published by ENISA and the European Commission, including eleven official reports, three studies and relevant website publications. Annual activity reports with annexes were extensively used to assess ENISA's performance. For certification schemes, published draft schemes for the EUCC and EUCS were reviewed to understand the state of play and barriers to adoption.

Academic literature review

Academic research was used to situate the evaluation within the broader European cybersecurity debate and to inform the initial focus of data collection. The literature provided critical perspectives on ENISA's epistemic authority, the challenges and vulnerabilities of the European cybersecurity domain and the alignment of the ECCF with international standards and best practices. Comparative

studies with other certification schemes were also reviewed to assess the competitiveness and adaptability of the ECCF.

3. Stakeholder consultation

Interview programme

The interview programme was a central pillar of the evaluation, designed to capture a wide range of perspectives from across the EU cybersecurity ecosystem. In total, 182 individuals were contacted (40 for ECCF, 142 for ENISA), resulting in 52 interviews for ENISA and 13 for ECCF. All interviews included questions on both ENISA and ECCF and 19 stakeholders were selected from survey respondents who volunteered for interviews.

ENISA: 52 interviews were conducted, involving ENISA staff, representatives from DG CNECT, DIGIT, INTPA, NEAR, other EU entities, industry, academia, international representatives and Member State officials.

ECCF: 13 interviews were conducted with 31 interviewees, including EU institutions, ECCG members and SCCG members. Despite challenges in engaging private stakeholders (only three of nine SCCG members responded), the analysis of stakeholder consultation data helped offset this limitation.

Survey programme

The survey approach was adapted after the inception report: instead of two separate surveys for internal and external stakeholders, an integrated survey was conducted to address all stakeholder groups. The survey included specific sections on ENISA and the ECCF, with question filtering and branching to ensure relevance.

- **Design:** The survey was developed based on desk research and initial interviews. It included both closed and open questions, with a limited number of mandatory items.
- **Dissemination:** Conducted via EUSurvey, 856 stakeholders received a personal invitation. The Commission and ENISA promoted the survey through various channels and the deadline was extended to maximise responses.
- **Results:** 209 responses were collected, with 70 respondents (33%) involved with the ECCF. The survey results were analysed using data science and analytics software, supplemented by manual analysis.

4. Workshops and validation activities

SWOT and recommendations workshops

SWOT workshop: held online on 21 May 2024 with 32 participants, including experts from academia, ENISA and the Commission. The workshop aimed to develop a SWOT analysis for ENISA and the ECCF, validate preliminary findings and foster technical exchange. Interactive polling and breakout sessions were used to gather and validate stakeholder input. The results were used to refine the strengths, weaknesses, opportunities and threats identified for both ENISA and the ECCF.

Recommendations workshop: held online on 12 July 2024 with 77 participants. The workshop presented preliminary evaluation results and facilitated collaborative discussions on lessons learned and potential improvements for ENISA and the ECCF. Interactive polls and an anonymous form to be filled by each Member State were used to collect feedback and validate findings.

Validation and quality assurance

The evaluation process included multiple validation steps to ensure the reliability and robustness of the findings:

- preliminary findings were presented to stakeholders in workshops, where interactive polling and open discussion allowed for real-time validation and refinement;
- an anonymous asynchronous feedback form was provided to capture additional input from stakeholders unable to participate in real time;
- the iterative process of presenting, discussing and refining findings ensured that the analysis accurately reflected the collective insights and perspectives of all participants.

5. Analytical approaches and quality assurance

The evaluation combined qualitative and quantitative methods, including desk research, literature review, stakeholder interviews, surveys and workshops. Data analysis was supported by analytics software and manual review. Quality was ensured through:

- iterative validation with stakeholders and expert input during workshops;
- systematic triangulation of data sources to cross-check findings;
- adaptation of tools (e.g. survey design) to maximise relevance and response rates.

6. Limitations and mitigating measures

- **Data and timing:** the main limitation was the difficulty in securing interviews with private stakeholders, particularly SCCG members. This was mitigated by analysing stakeholders' consultation data and extending the survey deadline.
- **Reliability:** the use of multiple data sources and triangulation of findings enhanced the reliability of the evaluation. Validation through stakeholder workshops and polling further strengthened the robustness of the conclusions.
- **Uncertainty:** some results, especially regarding the ECCF (where only one scheme was adopted by early 2024), are preliminary. The robustness of findings was enhanced by cross-referencing multiple sources and validating with stakeholders, but some uncertainty remains due to the evolving nature of the policy landscape.

7. Points of comparison

The main point of comparison for the evaluation was the baseline scenario of 2017, reconstructed from the 2017 Impact Assessment for the Cybersecurity Act and supporting studies. This baseline included ENISA's status and resources, the certification landscape, market and economic data and stakeholder perceptions. All comparisons and assessments were made against this baseline, as set out in the original evaluation roadmap.

8. Critical assessment of the contractor

The contractor's evaluation of ENISA demonstrated a certain positive bias, largely attributed to interviews with ENISA staff constituting a significant part of the interviews overall. While the report rightly acknowledges ENISA's resource constraints, the analysis could be more balanced regarding other areas for improvement. The study was improved following feedback from DG CONNECT in several instances.

ANNEX III. EVALUATION MATRIX AND, WHERE RELEVANT, DETAILS ON ANSWERS TO THE EVALUATION QUESTIONS (BY CRITERION)

This annex presents the evaluation matrix that serves as the central organising framework for the assessment of ENISA and the ECCF. It provides detailed, criterion-based responses to the evaluation questions, covering all five evaluation criteria: **effectiveness**, **efficiency**, **coherence, relevance** and **EU added value**.

The evidence and analysis included in this annex substantiate the findings outlined in Section 4 of the main evaluation report. For clarity and transparency, the questions and their corresponding evidence-based answers are presented individually and grouped by evaluation criterion. The depth of coverage for each criterion reflects its relative importance and the extent of supporting evidence available in the main body of the report.

Findings are presented separately for ENISA and the ECCF to reflect their distinct roles and contributions within the broader cybersecurity landscape.

1. Evaluation matrix:

The following sections present refined and up-to-date evaluation matrices used to assess the effectiveness, impact, efficiency, coherence, relevance and EU added value of both ENISA and the ECCF. These matrices are aligned with the latest edition of the European Commission's Better Regulation Guidelines and outline the evaluation questions (EQs) and operational questions (OQs), along with the corresponding judgement criteria, stakeholder groups and indicators used to evaluate each criterion.

The matrices also specify the data sources required to determine the values of the proposed indicators. Certain EQs and OQs have been specifically designed to address aspects unique to the ECCF.

Functioning as a structured analytical tool, the evaluation matrices demonstrate how evidence collected through various methodologies and data sources contributes to answering the evaluation questions and shaping the overall conclusions.

Effectiveness and impact

In line with the Better Regulation Toolbox, the effectiveness analysis examined how successfully ENISA and the ECCF have achieved or made progress toward their intended objectives. This involved assessing the actual outputs, results and impacts in relation to the goals of the action.

The effectiveness analysis yielded insights into the progress made so far by ENISA and the ECCF. The evaluation drew heavily on the intervention logic of both entities.

The tables below illustrate the structure of the evaluation matrix. Where appropriate, findings are presented separately for ENISA and the ECCF.

ENISA

Effectiveness **EQ1, ENISA**	**To what extent has ENISA achieved its objectives and implemented the tasks set out in its mandate? What, if anything, could be done to render ENISA more effective in achieving these objectives?**
OPERATIONAL QUESTIONS ▪ OQ1: Did the activities of ENISA result in the expected outputs? To what extent were the stakeholders satisfied with their quality? ▪ OQ2: To what extent has ENISA become a centre of expertise on cybersecurity? Where relevant, what were the main factors limiting ENISA's contribution to this objective? ▪ OQ3: To what extent has ENISA provided guidance, advice and assistance on cybersecurity policy development and implementation for MS and EU institutions? To what extent have ENISA's stakeholders followed the cybersecurity requirements issued by ENISA? ▪ OQ4: To what extent has ENISA enhanced MS capabilities in preventing and responding to cyber threats? Where relevant, what were the main factors limiting ENISA's contribution to this objective? ▪ OQ5: To what extent has ENISA's reputation in cybersecurity matters remained stable?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: Successful implementation of activities and delivery of outputs as a key precondition for achieving objectives	Number and share of successfully implemented activities and delivered outputs
OQ2: Stakeholders identify ENISA as a leading centre of expertise on cybersecurity	Share of stakeholders by group that considers ENISA to be a leading centre of expertise on cybersecurity
OQ3: Stakeholders identify ENISA as a leading partner in cybersecurity policy development and implementation	Share of stakeholders by group that considers ENISA to be a leading partner in cybersecurity policy development and implementation Share of stakeholders that adopted regulatory or managerial change as a result of ENISA's support
OQ4: MS representatives agree that ENISA provided crucial support in preventing and responding to cyber threats, including via the Cybersecurity Support Action	Share of MS representatives by country that considers ENISA to be a crucial provider of cybersecurity support in preventing and responding to cyber threats Share of MS stakeholders that considers the Cybersecurity Support Action effective; number and share of completed *ex ante* and *ex post* activities
OQ5: ENISA's reputation remained stable over the evaluation period	Perceptions of stakeholders about ENISA's work (two thirds of stakeholders assess ENISA's reputation in a positive way)
DATA SOURCES ▪ Desk research ▪ Interviews ▪ Survey ▪ Case studies ▪ Workshop on the intervention logic	

Effectiveness **EQ2, ENISA**	**To what extent has the governance framework been effective?**
OPERATIONAL QUESTIONS	
▪ OQ1: How effectively have the current governance, internal organisational structure and human resources policies and practices of ENISA contributed to its effectiveness? ▪ OQ2: Were the internal mechanisms for programming, monitoring, reporting and evaluating ENISA effective?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: ENISA's governance structure is conducive to the effectiveness of its work	ENISA's stakeholders consider its governance structure effective; ENISA fulfils its annual activities and objectives and complies with the management target scores
OQ2: The internal mechanisms for programming, monitoring, reporting and evaluating ENISA were effective	ENISA follows rules and procedures imposed by the Commission; ENISA staff considers the monitoring system effective; EC officials consider ENISA's internal monitoring system effective
▪ **DATA SOURCES** ▪ Desk research ▪ Interviews ▪ Survey	

Evaluation results
ENISA successfully fulfilled its mandate by delivering most planned outputs, even during challenging times like the COVID-19 pandemic and Russia's war of aggression against Ukraine. ENISA's effectiveness is largely due to its strong governance and matrix-based organisational model, which aids task delivery and cooperation. However, key areas for improvement have been identified, particularly in strategic prioritisation and resource allocation. Despite a solid governance structure, ENISA experiences delays due to resource constraints and rigid strategic plans, signalling a need for more agile management. Enhancing task prioritisation and aligning operational capacity with strategic objectives could bolster ENISA's efficiency and responsiveness to emergent cybersecurity challenges. The evaluation shows the need for additional resources. Additionally, more streamlined internal governance and dynamic reallocation of tasks and resources could help, to a certain extent, with timely fulfilment of new requests. Lastly, strengthened communication channels and a better-defined communication strategy would support ENISA's outreach to its public and private stakeholders.

ECCF

Effectiveness **EQ3, ECCF**	**To what extent has the ECCF achieved its objectives?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent has the ECCF increased capabilities and preparedness of Member States and businesses, in particular regarding critical infrastructures? ▪ OQ2: To what extent has the ECCF improved cooperation and coordination across Member States and EU institutions, agencies and bodies as well as well as with other relevant stakeholders (e.g. industry, standardisation bodies)? ▪ OQ3: To what extent has the ECCF improved EU-level capabilities to support and complement the action of Member States? ▪ OQ4: To what extent has the ECCF enhanced trust and awareness among the general public and businesses on cybersecurity issues through transparent information? ▪ OQ5: To what extent has the ECCF increased the overall transparency of cybersecurity assurance of ICT products and services, ensuring security by default and design as well as mitigation of vulnerabilities? ▪ OQ6: To what extent has the ECCF ensured that businesses can sell secure ICT products, services and processes across the internal market at lower administrative and financial costs? ▪ OQ7: To what extent has the ECCF reduced fragmentation of certification schemes in the EU and related security requirements and evaluation criteria across Member States and sectors?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: All Member States appointed national cybersecurity certification authorities	Number of national cybersecurity certification authorities appointed; resources allocated to national cybersecurity certification authorities
OQ1: ICT products, services or processes certified under the EU cybersecurity certification schemes	Number of certification schemes issued and businesses certified
OQ2: ECCG set up and taking decisions	Number of ECCG meetings that took place; type of issues discussed; number and type of decisions taken and documents adopted
OQ2: Certificates issued under the 'Senior Officials Group Information Systems Security - Mutual Recognition Agreement' (SOG-IS-MRA) extended to the EU27 in view of an equivalent EU scheme	Number of SOGIS-MRA equivalent schemes at EU level, extended to EU27; number and type of decisions taken and documents adopted by the SOG-IS MRA and transferred to EU level
OQ3: ENISA has more resources to tackle cybersecurity certification issues	Resources effectively allocated to ENISA (number of staff and financial endowment) to carry out certification-related tasks
OQ4: More people and businesses know about cybersecurity certification	Percentage of the general public and businesses aware of cybersecurity certification; percentage of the general public and businesses aware of the importance of a high level of security of ICT products, services and processes

OQ5: Buyers, in particular operators of essential services, are more incentivised to purchase certified ICT products, services and processes compared to before the Cybersecurity Act	Extent to which the ECCF has contributed to the purchase of certified ICT products, services and processes
OQ6: Vendors are more incentivised to certify their ICT products, services and processes compared to before the Cybersecurity Act	Extent to which the ECCF has contributed to the certification of ICT products, services and processes
OQ7: Less or no cybersecurity certification schemes were developed outside the perimeter of the ECCF compared to before its adoption	Number and type of cybersecurity certification schemes developed outside the ECCF perimeter
DATA SOURCES ▪ Desk research ▪ Interviews ▪ Survey ▪ Workshop on the intervention logic	

Effectiveness **EQ4, ECCF**	**What are the main gaps and challenges that have hindered the achievement of the objectives of the ECCF? Why?**
OPERATIONAL QUESTIONS ▪ OQ1: Which administrative shortcomings have prevented the ECCF from achieving its objectives? Did these shortcomings appear or increase during the COVID-19 pandemic, following geopolitical tensions or the emergence of other EU policy priorities? ▪ OQ2: Which legal shortcomings have prevented the ECCF from achieving its objectives? Did these shortcomings appear or increase during the COVID-19 pandemic, following geopolitical tensions or the emergence of other EU policy priorities? ▪ OQ3: Which operational shortcomings have prevented the ECCF from achieving its objectives? Did these shortcomings appear or increase during the COVID-19 pandemic, following geopolitical tensions or the emergence of other EU policy priorities?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: Administrative barriers, such as time-consuming procedures and lack of effective decision-making tools as well as conflicting national certification procedures/requests	Number of administrative procedures initiated and finalised; type of shortcomings in decision-making highlighted by participants in the ECCF (in particular ENISA, Member States and the Commission)
OQ2: Legal barriers, such as national legal frameworks and requirements hindering the adoption of EU cybersecurity certification schemes	Number of initiated and finalised legal acts, including implementing law, at both EU and national level; type of shortcomings highlighted by participants in the ECCF (in particular ENISA, Member States and the Commission, SCCG members)
OQ3: Operational barriers, such as the lack of online platforms and adequate collaboration tools	Number and type of exchanges allowed by existing collaboration tools; type of shortcomings in operational tools highlighted by participants in the ECCF (in particular ENISA, Member States and the Commission)
DATA SOURCES ▪ Desk research ▪ Interviews	

▪ Survey

Evaluation results
The ECCF made a modest contribution to enhancing the cybersecurity capabilities of Member States and private companies. National authorities recognised the ECCF's support in developing national cybersecurity certification capabilities but highlighted significant resource disparities between Member States. ENISA reported staffing difficulties, mainly related to turnover and the limited number of personnel available to carry out all activities arising from new schemes, including in Member States. Delays in the adoption of certification schemes caused by disagreements between Member States, legal complications, politicisation and coordination issues, negatively affected the ECCF's effectiveness, thus impacting the achievement of its objectives. Despite these obstacles, the ECCF strengthened cooperation and coordination between Member States and EU institutions in cybersecurity certification.

Efficiency

Efficiency-related questions examine the resources invested in relation to the changes generated by the measure. This involves assessing the inputs against the outputs, results and impacts, essentially weighing costs against benefits. The efficiency evaluation explored the costs associated with the EU measure as they affect various stakeholder groups, along with the factors influencing these costs and their connection to ENISA and the ECCF.

This evaluation was conducted based on the outcomes experienced by different stakeholder groups, as identified in the effectiveness analysis. Where feasible, these outputs were quantified. The analysis also acknowledged that while costs may initially outweigh benefits, net benefits could emerge over time, particularly given ENISA's recently extended mandate and the early-stage development of the ECCF.

The overall conclusions drawn from the efficiency questions provided insight into whether the resources allocated to ENISA's activities and the implementation of the ECCF are being used optimally and are necessary to achieve the measure's objectives. Where findings indicated inefficiencies, opportunities for simplification and burden reduction were identified and examined. Where applicable, the evaluation also highlighted areas with the potential for improving efficiency and streamlining the design and implementation of the measure.

The tables below outline the structure of the evaluation matrix. Findings are presented separately for ENISA and the ECCF.

ENISA

Efficiency **EQ1, ENISA**	**To what extent has ENISA been efficient in implementing the tasks set out in its mandate as laid down in its Regulation?**
OPERATIONAL QUESTIONS	
▪ OQ1: Have the resources allocated to ENISA been sufficient for the pursuit of its tasks (input/output analysis)? To what extent has the execution of the tasks been effectively resourced? ▪ OQ2: Were the annual budgets of ENISA implemented in an efficient way considering the results achieved?	

JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The extent to which the resources allocated to ENISA have been sufficient for the pursuit of its individual tasks	Title II commitment and paid budget share; opinions of ENISA staff and EC officials on the extent to which individual tasks were effectively resourced
OQ2: The annual budget of ENISA has been implemented efficiently	ENISA commitment and paid budget; annual budget implementation targets
DATA SOURCES	
▪ Desk research ▪ Interviews	

Efficiency **EQ2, ENISA**	**To what extent has ENISA adapted to periods of high workload?**
OPERATIONAL QUESTIONS	
▪ OQ1: What were the periods of high workload during the evaluation period? ▪ OQ2: Did ENISA manage to carry on with all their tasks during these periods?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The high workload periods identified	The periods of high workload are analysed where relevant
OQ2: Tasks were implemented during the period of high workload	Findings of other evaluation questions indicate that ENISA kept performing its tasks during the period of high workload
DATA SOURCES	
▪ Desk research ▪ Interviews ▪ Survey	

Efficiency **EQ3, ENISA**	**To what extent have ENISA's internal organisation, governance and procedures been conducive to its efficiency and what administrative costs and burdens do they create and for whom?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent do ENISA's internal organisation, governance and procedures support its ability to perform its tasks, given its mandate and size? ▪ OQ2: How does the balance of operational staff and administrative support staff affect the implementation of ENISA's tasks and the achievement of its objectives?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The extent to which ENISA's internal organisation, governance and procedures are fit for purpose without excessive costs and major administrative burdens	Alignment of ENISA's internal organisation, governance and procedures with its mandate and size; the volume of administrative costs and administrative burdens; IAS and ECA opinions on the governance of ENISA

OQ2: The balance between operational and administrative support staff is appropriate	Number and share of administrative and operational staff; staff performance management indicators; qualitative opinion of interviewed staff members
DATA SOURCES ▪ Desk research ▪ Interviews ▪ Survey	

Efficiency **EQ4, ENISA**	**What aspects, means, actors or processes render ENISA more or less efficient?**
OPERATIONAL QUESTIONS ▪ OQ1: What are the inefficiencies identified in ENISA's activities? ▪ OQ2: Which of ENISA's activities are particularly efficiently or inefficiently implemented?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: ENISA addressed all identified inefficiencies	Findings on the previous efficiency questions and stakeholder perceptions
OQ2: Good and bad practices identified in the selected activities	
DATA SOURCES ▪ Desk research ▪ Interviews ▪ Case studies	

Evaluation results
The evaluation highlighted that while ENISA operated efficiently under its governance structure, it struggled with increasing demands and filling specialised positions due to a global IT and cybersecurity specialist shortage and insufficient resources, resulting in task delays and periods of high stress for personnel. Improvements can be made to a certain extent by optimising internal workforce management to handle critical tasks, as demonstrated by reallocating 10.5 FTEs for the Cybersecurity Support Action. Additionally, enhancing budget and procurement management could improve internal efficiency and address the downward trend in balancing appropriations. Although ENISA's budget grew significantly between 2017 and 2023, it continued to face resource constraints that impacted its operational efficiency.

ECCF

Efficiency **EQ5, ECCF**	**To what extent has the ECCF been implemented efficiently?**
OPERATIONAL QUESTIONS	

- OQ1: What benefits have been experienced by Member States since the establishment of the ECCF?
- OQ2: What costs have been borne at national level since the establishment of the ECCF?
- OQ3: What benefits have been experienced at EU level (i.e. Commission, ENISA) since the establishment of the ECCF?
- OQ3: What costs have been borne at EU level (i.e. Commission, ENISA) since the establishment of the ECCF?
- OQ4: What benefits have been experienced by businesses and the general public since the establishment of the ECCF?

JUDGEMENT CRITERIA AND INDICATORS

OQ1: Member States confirm they experienced a set of benefits as a result of participating in the ECCF, especially compared to SOG-IS-MRA	Benefits from participating in, and issuing certificates valid under, the SOG-IS-MRA; benefits from participating in the ECCF
OQ2: Member States confirm they incurred a set of costs as a result of participating in the ECCF	Costs, including administrative and human resources costs, borne as a result of implementing the ECCF at national level (Member States), including the establishment of national certification authorities
OQ3: Commission and ENISA confirm they experienced a set of benefits as a result of participating in the ECCF, especially compared to SOG-IS-MRA	Benefits from participating in, preparing and adopting certification schemes
OQ3: Commission and ENISA confirm they incurred a set of costs as a result of participating in the ECCF	Costs, including administrative and human resources costs, borne as a result of implementing the ECCF at EU level (Commission, ENISA)
OQ4: Businesses and the general public confirm they experienced a set of benefits deriving from the ECCF	Benefits in terms of competitiveness for businesses; benefits in terms of more awareness for the general public

DATA SOURCES

- Desk research
- Interviews
- Survey

Efficiency **EQ6, ECCF**	**What aspects, means, actors or processes render the ECCF more or less efficient?**

OPERATIONAL QUESTIONS

- OQ1: What are the inefficiencies identified in the ECCF's processes or outputs?
- OQ2: What ECCF activities or processes are particularly efficiently implemented? To what extent have the adoption of the Union Rolling Work Programme, the preparation of schemes carried out by ENISA, the opinions provided by the ECCG, advice provided by the SCCG and ad-hoc working groups contributed to the smooth functioning of the ECCF?
- OQ3: What are the factors that could be linked to each of the elements that demonstrate efficiencies and inefficiencies?

JUDGEMENT CRITERIA AND INDICATORS

OQ1: There are no identified inefficiencies	Findings on the previous efficiency questions and stakeholder perceptions triangulated with additional data sources.
OQ2: Identified good practices in the selected activities	
OQ3: Causal factors of efficient and inefficient practices are identified	

DATA SOURCES
▪ Desk research ▪ Interviews ▪ Survey

Evaluation results
The efficiency of the ECCF was shaped primarily by challenges related to both the substance and the procedures involved. Issues concerning content included political factors and the technical complexity of the certification schemes, which varied depending on the stakeholders and the specific products or services subject to certification. Procedural difficulties arose from preparation and adoption processes that had not been previously tested and were potentially cumbersome. On the other hand, the voluntary nature of the schemes did not seem to have a notable influence on the ECCF's efficiency. The formation of dedicated groups and forums facilitated necessary stakeholder involvement even though there remains substantial room for organisational improvement and refinement of internal governance.

Coherence

The coherence analysis examined the extent to which the objectives of ENISA and the ECCF align with and complement other initiatives and the work of EU and national bodies in the field of cybersecurity. Specifically, the external coherence analysis assessed how well ENISA and the ECCF support the broader cybersecurity policy goals of the European Commission.

Internal coherence was also evaluated to determine how effectively the various components within ENISA and the ECCF function together to achieve their respective objectives.

The tables below present the structure of the evaluation matrix. Where relevant, findings are presented separately for ENISA and the ECCF.

ENISA

Coherence **EQ1, ENISA**	**How well has ENISA supported the overarching policy goals?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent has ENISA contributed to the implementation of the NIS2 Directive?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: ENISA positively contributed to the implementation of the NIS2.	Quality of implementation of NIS2 provisions.

DATA SOURCES
▪ Desk research ▪ Interviews ▪ Survey

Coherence **EQ2, ENISA**	**To what extent has ENISA fostered cooperation at EU and national level?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent has ENISA exploited synergies in expertise and knowledge sharing with other stakeholders and EU/MS bodies and private and public stakeholders? ▪ OQ2: To what extent has ENISA coordinated its work with other EU/national bodies and private and public stakeholders in preventing and responding to cyber threats?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: ENISA sufficiently exploited synergies in expertise and knowledge sharing with other stakeholders and EU/MS bodies	Opinions of stakeholders (with two thirds of all stakeholders having a positive opinion); share of synergies exploited and their contribution to the quality of achieved outputs
OQ2: ENISA made the best use of existing resources while working with other EU/national bodies and private and public stakeholders in preventing and responding to cyber threats (while avoiding overlaps)	Share of complementarities and overlaps in the work of ENISA with other EU/national bodies[16]; opinions of stakeholders on this issue (with two thirds of all stakeholders having a positive opinion)
OQ3: Stakeholders confirm ENISA's leading role in the cooperation between MS, EU institutions, companies and other groups in the cyber domain	Share of stakeholders by group and country that considers ENISA's role in maintaining cooperation among them as crucial
DATA SOURCES	
▪ Desk research ▪ Interviews ▪ Survey	

Evaluation results
The findings reveal that ENISA played a proactive role in encouraging collaboration and the exchange of knowledge among stakeholders. While ENISA effectively promotes cybersecurity cooperation across the EU, there is room for improvement in streamlining operations and enhancing synergies with EU bodies like the ECCC and national authorities. Formalising cooperation with agencies such as EMSA and the JRC could make for a more unified approach to cybersecurity initiatives. Furthermore, refining internal communication and clarifying ENISA's role in policy implementation could improve efficiency and regulatory consistency.

[16] Other EU and national bodies working on cybersecurity and digital privacy include various Commission directorates, the European External Action Service and other EU bodies and agencies such as BEREC, EUROPOL and CERT-EU, national cybersecurity competent authorities or regulators, national CSIRTs/Computer Emergency Response Teams and more recently the European Cybersecurity Competence Centre (ECCC) and its network of national coordination centres (NCCs).

ECCF

Coherence **EQ3, ECCF**	**To what extent is the ECCF coherent or overlapping with other relevant initiatives in the area of cybersecurity market?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent is the ECCF coherent and complementary with other policy, legal and funding instruments adopted at EU and national level? ▪ OQ2: To what extent does the ECCF overlap or create gaps with other policy, legal and funding instruments adopted at EU and national level?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The ECCF's scope complements that of other EU and national instruments	Extent to which the ECCF complements EU measures that have already been adopted (i.e. NIS2 Directive, European Cybersecurity Competence Centre and Network, Digital Europe programme) or that have been proposed (i.e. Cyber Resilience Act, Cyber Solidarity Act); extent to which the ECCF complements national cybersecurity certification measures adopted since the entry into force of the Cybersecurity Act; share of Member States detecting complementarity
OQ2: Other EU and national instruments tackle different aspects of securing the cybersecurity of ICT products, services and processes	Extent to which the ECCF scope overlaps with EU measures adopted (i.e. NIS2 Directive, European Cybersecurity Competence Centre and Network, Digital Europe programme) or proposed (i.e. Cyber Resilience Act, Cyber Solidarity Act); extent to which the ECCF scope overlaps with national cybersecurity certification measures adopted since the entry into force of the Cybersecurity Act; share of Member States detecting complementarity
DATA SOURCES	
▪ Desk research ▪ Interviews ▪ Survey	

Coherence **EQ4, ECCF**	**To what extent is the ECCF coherent internally?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent are the various elements of the ECCF coherent among themselves?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The ECCF procedures, governance mechanisms and working arrangements are coherent among themselves	Number and type (e.g. legal, administrative, operational) of issues identified by ENISA, the Commission and relevant forums (i.e. ECCG, SCCG, ad hoc working group members)
DATA SOURCES	
▪ Desk research ▪ Interviews ▪ Survey	

Coherence **EQ5, ECCF**	**To what extent is the ECCF coherent with other EU-level actions, particularly sectoral ones, in the area of certification?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent does the ECCF complement or overlap with EU policies in the area of certification? ▪ OQ2: To what extent is the ECCF coherent with the EU digital strategy and other relevant sectoral strategies?	
JUDGEMENT CRITERIA AND INDICATORS	
Other EU initiatives (e.g. delegated act under Radio Equipment Directive, etc.) to secure/certify ICT products, services and processes do not overlap with the ECCF	Number and type of sectoral EU policies implemented; extent to which the sectoral policies overlap with the ECCF
The ECCF ensures trust in ICT products, services and processes that otherwise would not be covered by other cybersecurity requirements	Number and type of digital strategy actions and sectoral strategies implemented; extent to which digital strategy actions and sectoral strategies overlap with the ECCF
DATA SOURCES	
▪ Desk research ▪ Survey ▪ Interviews	

Evaluation results
While theoretically consistent with EU legal measures on cybersecurity, in particular the CRA (proposal at the time of the evaluation) and the NIS2 Directive, the ECCF has been found to lack clear accountability mechanisms ensuring consistency with the existing EU legal framework and requiring diligent oversight. The CRA (under development) is expected to considerably impact the legal framework related to the security evaluation and certification of ICT products. In this regard, the forthcoming implementation of the EUCC scheme will significantly test its coherence with the existing EU legal framework.

EU added value

In accordance with the Better Regulation Toolbox, the assessment of EU added value focused on identifying changes resulting from the activities of ENISA and the ECCF that would not likely have occurred through actions taken solely by Member States. The evaluation considered the factors contributing to EU added value, such as enhanced coordination, improved effectiveness or efficiency and reduced administrative burden, among others.

The tables below outline the structure of the evaluation matrix. Findings are presented separately for ENISA and the ECCF.

ENISA

EU added value **EQ1, ENISA**	**Could the identified outputs, results and impacts have been achieved without EU intervention?**
OPERATIONAL QUESTIONS ▪ OQ1: What other possible options are there for achieving the outputs and results? ▪ OQ2: Is it still valid to assume that the objectives of the action can best be met by action at EU level?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: Feasibility of alternative options for achieving the outputs and results of ENISA	List of alternative options and their description
OQ2. EU-level action is considered the most optimal	Stakeholders' opinions on the added value of ENISA
DATA SOURCES ▪ Desk research ▪ Interviews	

EU added value **EQ2, ENISA**	**What would be the most likely consequences of stopping or withdrawing EU involvement?**
OPERATIONAL QUESTIONS ▪ OQ1: How would the EU cybersecurity landscape change if EU involvement were to be withdrawn or stopped? ▪ OQ2: What would stakeholders see as a suitable alternative to the current EU action?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: Anticipated quality of feasible alternative options	Stakeholders' opinions on the added value of ENISA
OQ2: Stakeholders see ENISA as the most optimal option	
DATA SOURCES ▪ Desk research ▪ Interviews	

Evaluation results
The achievements in terms of outputs, results and impacts would have been difficult to attain without ENISA's involvement. ENISA's dedicated focus on the implementation of cybersecurity policy, combined with its ability to coordinate and align efforts across Member States, represents a unique contribution that other EU bodies may not be able to provide due to their broader mandates or more narrowly defined roles. ENISA brought added value to EU cybersecurity through its independent and decentralised structure, which enhanced cooperation with Member States and supported responses to cybersecurity threats. Without ENISA, the EU would likely encounter greater difficulties in coordinating efforts across borders and would face a more fragmented cybersecurity landscape, particularly affecting those Member States with less advanced capabilities in this field. Strategically increasing stakeholder engagement and reassessing resources could help ENISA better adapt to evolving cybersecurity threats and expand its operational role. Future priorities include improving

recruitment processes, managing workload and strengthening transparent relationships with Member States to enhance cooperation and information sharing. Addressing criticism from private-sector stakeholders by tailoring insights to their specific challenges should also be considered.

ECCF

EU added value **EQ3, ECCF**	**To what extent has the ECCF brought EU added value compared to what could have been achieved by Member States alone?**
OPERATIONAL QUESTIONS	
▪ OQ1: Could the same outcomes of the ECCF be achieved by participating countries adopting cybersecurity certification schemes outside the European framework? ▪ OQ2: To what extent could Member States have achieved the same outcomes without the ECCF? ▪ OQ3: To what extent has the ECCF increased the likelihood of achieving a more secure, transparent and cohesive internal market for ICT products, services and processes?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: Member States state that they prefer to use the ECCF to achieve a harmonised, streamlined and coherent cybersecurity certification mechanism	Number of Member States preferring to use the ECCF; number and type of parallel certification procedures carried out by Member States
OQ2: Member States' unilateral and uncoordinated measures were ineffective in securing ICT products, services and processes placed on the internal market	Number of national certification measures successfully certifying ICT products, services and processes; number of certification procedures carried out under the SOG-IS-MRA
OQ3: ECCF increases the security of ICT products, services and processes sold in the internal market	Extent to which the certification of ICT products, services and processes through the ECCF has guaranteed more security
DATA SOURCES	
▪ Desk research ▪ Survey ▪ Interviews	

Evaluation results
Stakeholders generally agreed that the ECCF delivers added value at EU level beyond what individual Member States could achieve on their own, even though its direct impact remains limited. This added value was particularly noticeable in areas such as the adoption of certification, the use of cost-efficient procedures, the promotion of cyber-awareness, the strengthening of trust within the EU single market and the encouragement of cybersecurity principles by default and by design. Most stakeholders also acknowledged the ECCF's role in contributing to a more secure, transparent and unified internal market for ICT products, services and processes. However, the added value of the ECCF has been somewhat limited due to its shortcomings in reaching its objectives (see effectiveness criteria) and its lack of efficiency (see efficiency criteria).

Relevance

According to the Better Regulation Toolbox, the relevance evaluation compared the needs and challenges present at the time of the adoption of Regulation (EU) 2019/881, which established ENISA's current mandate and the European cybersecurity certification scheme, with those encountered during its

implementation. The evaluation also examined how the current and anticipated future needs and problems within the EU align with the objectives of ENISA and the ECCF.

The relevance evaluation identified potential mismatches between the objectives of ENISA and the ECCF and the evolving cybersecurity landscape. For instance, some of the 'problem drivers' outlined in the original impact assessment may no longer be applicable, while emerging technological developments could introduce new challenges related to cybersecurity innovation.

The tables below outline the structure of the evaluation matrix. Findings are presented separately for ENISA and the ECCF.

ENISA

Relevance **EQ1, ENISA**	**Are objectives and tasks revisited periodically to identify upcoming and urgent needs?**
OPERATIONAL QUESTIONS	
▪ OQ1: How flexible has ENISA been in adapting to the evolving landscape of threats, regulatory changes and policy responses? Where relevant, what were the main factors limiting ENISA's contribution to this objective?	
JUDGEMENT CRITERIA AND INDICATORS	
ENISA quickly adapted to the evolving landscape of threats, regulatory changes and policy responses	Speed of organisational responses to the changing regulatory environment and policy responses; speed and quality of responses to emerging cyber threats
DATA SOURCES	
▪ Desk research ▪ Interviews ▪ Survey	

Relevance **EQ2, ENISA**	**Did ENISA's objectives and tasks respond successfully to the overall EU policy objectives and the needs of stakeholders?**
OPERATIONAL QUESTIONS	
▪ OQ1: Has ENISA correctly identified the needs of its stakeholders and the EU policy objectives? ▪ OQ2: Has ENISA successfully responded to the needs of its stakeholders and the EU policy objectives?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The needs of ENISA's stakeholders and the EU policy objectives (including priorities) were duly identified.	Needs of stakeholders were acknowledged in ENISA's organisational decision-making; practices of stakeholder consultation have been duly established and implemented; positive perceptions of ENISA's stakeholders on those issues

OQ2: ENISA responded well to the needs of stakeholders and the EU policy objectives.	EU policy objectives (including priorities) in the field of cybersecurity were acknowledged and referred to in ENISA's documents
DATA SOURCES ▪ Desk research ▪ Interviews ▪ Survey	

RELEVANCE **EQ3, ENISA**	**To what extent has ENISA supported the Commission and Member States in their policy-related tasks?**
OPERATIONAL QUESTIONS ▪ OQ1: To what extent do ENISA's stakeholders indicate that the role and purpose of ENISA in policy-related tasks are clear and properly defined? ▪ OQ2: To what extent have ENISA's operations enabled Commission staff to better focus on the institutional tasks?	
JUDGEMENT CRITERIA AND INDICATORS	
EC officials consider ENISA's operation optimal for its institutional tasks.	Opinion of EC officials on the operation of ENISA; IAS, ECA evaluations Perception of ENISA's stakeholders (two thirds of surveyed/interviewed stakeholders have a positive opinion on the specific aspects of ENISA's performance)
ENISA's stakeholders view its policy development support positively.	
ENISA's stakeholders view its policy implementation support positively.	
ENISA's stakeholders view ENISA's advice and opinion positively.	
DATA SOURCES ▪ Desk research ▪ Interviews ▪ Survey	

Evaluation results
ENISA's significance in the cybersecurity domain is highlighted by its adaptability to evolving stakeholder needs and its ability to realign its focus to meet emerging developments. ENISA reacted successfully to changes in the cybersecurity environment, resulting in high levels of satisfaction among stakeholders. However, some expressed concerns about ENISA's ability to fully address the rising cyber threats across Europe. National cybersecurity bodies and smaller Member States benefited from ENISA's initiatives in building capacity and providing regulatory guidance. Nonetheless, there remain opportunities to strengthen ENISA's relevance, particularly by taking a more proactive role in offering tools and support tailored to specific sectors. This is especially important for small and medium-sized enterprises (SMEs), which face distinct needs and challenges. By revisiting

priorities, improving its communication, streamlining processes, ensuring adequate resources and, to a certain extent, efficiently utilising existing resources, ENISA can strengthen its foundational role within Europe's cybersecurity framework and better align with the dynamic demands of the European cybersecurity landscape.

ECCF

Relevance **EQ4, ECCF**	**To what extent are the scope and objectives of the ECCF still relevant?**
OPERATIONAL QUESTIONS	
▪ OQ1: To what extent are the objectives of the ECCF still relevant for addressing the cybersecurity threat landscape? ▪ OQ2: To what extent are the objectives of the ECCF still relevant considering how the EU policy context has changed since its adoption?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The ECCF is still needed to tackle cybersecurity threats to the EU.	Number of ECCF objectives which are still relevant in the current threat landscape.
OQ2: The ECCF is still needed despite the EU policy and programmes implemented since its introduction.	Number of objectives which are still relevant after the introduction of the NIS2 Directive, the European Cybersecurity Competence Centre and Network, the EU cybersecurity strategy and the Digital Europe programme as well as the proposals for a CRA and a Cyber Solidarity Act.
DATA SOURCES	
▪ Desk research ▪ Interviews	

Relevance **EQ5, ECCF**	**To what extent is the ECCF still relevant in terms of achieving its objectives?**
OPERATIONAL QUESTIONS	
▪ OQ1: Are the features of the ECCF (schemes and procedures) envisaged in the Cybersecurity Act still relevant in terms of fulfilling its objectives in the current threat landscape? ▪ OQ2: To what extent is the ECCF relevant in terms of securing ICT products, services and processes? To what extent has it increased or decreased in relevance in view of increasing geopolitical tensions in digital policy?	
JUDGEMENT CRITERIA AND INDICATORS	
OQ1: The Commission and Member States do not highlight the need for adjustments to fulfil its objectives in the current threat landscape.	Extent of possible adjustments needed to tackle current cybersecurity threats.
OQ2: The relevance of the ECCF increased for Member States.	Number and type of cybersecurity certification initiatives launched, both in the EU and internationally since the adoption of the Cybersecurity Act; extent to which Member States state that cybersecurity certification is needed.

DATA SOURCES
▪ Desk research ▪ Survey ▪ Interviews

Evaluation results
The ECCF remains relevant in supporting the objectives of the internal market. Given the rising frequency and seriousness of cybersecurity threats, stakeholders considered EU cybersecurity certification to be a useful and important tool to enhance Europe's cyber resilience and preparedness. Several elements contributed to the ECCF's perceived relevance, including enhanced cooperation at EU level, assistance in the development of standards and the possibility of requiring certification for critical infrastructure (e.g. under NIS2) and recipients of public procurement. In addition, stakeholders pointed to the ECCF's ability to strengthen collaboration among EU Member States and promote trade by offering a harmonised certification platform.

ANNEX IV. OVERVIEW OF BENEFITS AND COSTS [AND WHERE RELEVANT, TABLE ON SIMPLIFICATION AND BURDEN REDUCTION]

Annex IV provides an overview of the costs and benefits projected in the preferred options of the 2017 CSA IA. It also shows the potential simplification and burden reduction savings identified in the current 2025 IA for the updated CSA preferred options. This annex presents a comparison, highlighting both the initial expectations and the most recent projections for the main policy options considered for ENISA and the ECCF. It is important to note that, at the time of this evaluation, there is no quantitative data available on the simplification or burden reduction already achieved for ENISA. For certification, no realised savings can be reported yet, as the first EU-wide certification scheme was only adopted in May 2025 and the evaluation was conducted between 2023 and 2024. As a result, the annex focuses on projected and potential impacts, rather than on realised monetary benefits or cost reductions for either ENISA or the ECCF.

Table 1. Overview of the costs and benefits identified in the evaluation

	Citizens/Consumers		**Businesses**		**Administrations**	
	Quantitative data	**Comment**	**Quantitative data**	**Comment**	**Quantitative data**	**Comment**
Costs						
Direct compliance costs (adjustment costs, administrative costs, regulatory charges)	No monetary costs were projected.	No direct compliance costs for citizens/consumers identified.	No monetary costs were projected.	No direct compliance costs for businesses in the short term, as certification remains voluntary.	**ENISA:** +EUR 9-12 million/year (to reach EUR 20-23 million/year); 50 additional staff (36 permanent, 14 external) (recurrent). **ECCF:** Member States: ~EUR 1.6 million/year per authority for personnel, equipment and	ENISA costs mostly borne by EU budget; ECCF costs for Member States relate to setting up and running certification authorities.

					operations (recurrent). **EU Commission:** 3 FTEs for scheme adoption (recurrent). **Expert group:** EUR 16 000-17 000/year (recurrent).	
Enforcement costs: (costs associated with activities linked to implementing an initiative, such as monitoring, inspections and adjudication/litigation)	No monetary costs were projected.	Not specified.	No monetary costs were projected.	Not specified for businesses.	**Member States:** ~EUR 290 000-300 000/year per authority for enforcement and supervision (recurrent).	Applies to operational management of certification authorities.
Indirect costs (indirect compliance costs or other indirect costs such as transaction costs)	No monetary costs were projected.	Not specified.	No monetary costs were projected.	Not specified for businesses	No monetary costs were projected.	Not specified.
Benefits						
Direct benefits (such as improved wellbeing, changes in pollution levels, safety, health, employment, market efficiency)	No monetary costs were projected.	Not directly quantified. Expected reduction in cyber incidents and improved trust and security (recurrent).	No monetary costs were projected.	Direct benefits from reduced investment in commercial analyses/reports; free access to ENISA outputs; improved competitiveness;	No monetary costs were projected.	Efficiency gains for EU budget; economies of scale in information collection and operational cooperation; reduced need for new EU body (saves

				reduced market-entry barriers for SMEs; and access to wider cybersecurity market (recurrent).		EUR 21.9 million in set-up costs) (one-off).
Indirect benefits (such as wider economic benefits, macroeconomic benefits, social impacts, environmental impacts)	No monetary costs were projected.	Not specified.	Expected reduction in costs of cybercrime incidents (currently ~0.41% of EU GDP, ~EUR 55 billion/year) (recurrent).	Indirect benefits from harmonised policy; reduced administrative burden; mutual recognition of certificates; increased trust in digital solutions; and improved access to public procurement (recurrent).	No monetary costs were projected.	Member States benefit from economies of scale, reduced duplication and more harmonised approaches.

PART II: II <u>Potential</u> simplification and burden reduction (savings)						
	Citizens/Consumers/Workers		**Businesses**		**Administrations**	
	Quantitative data	**Comment**	**Quantitative data**	**Comment**	**Quantitative data**	**Comment**
Description:						
Option A.2: Reform of ENISA's mandate	Attestation cost per attestation: ~EUR 300-350 (public) vs	Better visibility on the labour market for cybersecurity professionals; better career progression;	EUR 3.7 to 4.4 billion over five years (broad estimate) for faster	Reputation of skills attestation providers; access to the cybersecurity skills	Fees offset ENISA operational costs.	Cost avoidance for public authorities that are developing or plan to develop attestation schemes

	~EUR 677 (private).	better wages; increased portability of skills.	incident detection and response.	market (especially SMEs); improved incident response reduces breach costs; streamlined certification processes.		(reduced compliance and supervisory burden for authorities); use of national liaison officers for some tasks.
Option B.2: Reform the ECCF by revising procedures and extending scope to simplify regulatory compliance	No monetary savings were projected.	Faster access to certified services; indirect benefit from improved security and reduced incident costs.	N/A	Single certification instead of multiple national ones; reduced compliance costs; lower cyber insurance premiums; increased mutual recognition.	Reduced time to develop schemes.	Reduced supervisory burden; streamlined scheme adoption and monitoring.
Option C.2: Targeted action – further simplification of compliance with relevant EU cybersecurity legislative framework	No monetary savings were projected.	Reduced compliance costs for individuals in reclassified entities; indirect benefit from improved security and fewer incidents.	Annual savings in compliance costs of EUR 14.7 billion over five years.	Reduced administrative burden due to fewer entities in scope; streamlined demonstration of compliance via certification.	Annual savings in enforcement costs of EUR 7.5 million over five years.	Reduced supervisory burden for authorities; simplified compliance monitoring; 28 700 fewer NIS2 entities to be supervised.

ANNEX V. STAKEHOLDER CONSULTATION - SYNOPSIS REPORT

This annex summarises all the consultation activities carried out as part of the evaluation of ENISA and the ECCF. The consultation strategy was designed to collect input from all relevant stakeholder groups, including public authorities, EU institutions, industry, academia, civil society and individual citizens. It covers the full range of activities undertaken, such as the call for evidence, the targeted survey, targeted interviews and dedicated workshops. It provides a consolidated overview of stakeholder feedback on the performance, strengths, weaknesses and areas for improvement of ENISA and the ECCF. The evidence collected through these activities forms a key part of the analytical framework supporting the evaluation and informs the recommendations for future policy development.

1. Consultation scope and objectives

Scope

The stakeholder consultation activities were undertaken as part of the evaluation of ENISA and the ECCF, in accordance with Article 67 of Regulation (EU) 2019/881, known as the Cybersecurity Act. The evaluation covered the period from 2017 to 2023 and sought to assess the performance of ENISA and the ECCF against the criteria of effectiveness, efficiency, relevance, coherence and EU added value. The consultation activities were designed to gather evidence from a wide range of stakeholders in order to inform the evaluation and support evidence-based policy-making.

The consultation addressed both ENISA and the ECCF, focusing on ENISA's mandate, objectives, governance, working practices and the implementation of the ECCF. The scope included assessing ENISA's support for policy development and implementation, capacity building, stakeholder engagement, and the development and adoption of cybersecurity certification schemes under the ECCF.

Objectives

The objectives of the stakeholder consultation were as follows:

- to collect comprehensive and representative feedback from all relevant stakeholder groups regarding the performance, strengths, weaknesses and areas for improvement of ENISA and the ECCF;
- to assess the effectiveness, efficiency, relevance, coherence and EU added value of ENISA's activities and the ECCF, as perceived by stakeholders;
- to identify lessons learned and recommendations for potential changes to the existing Regulation and for improving the performance of ENISA and the ECCF;
- to ensure that the evaluation is informed by the experiences, needs and expectations of Member States, EU institutions, industry, standardisation bodies, academia, non-governmental organisations and other relevant actors;

- to gather input on the implementation and impact of the ECCF, including the development and adoption of certification schemes, stakeholder involvement, transparency and alignment with EU and international standards.

The consultation was structured in such a way as to provide evidence for the evaluation's analytical framework, which included a mixed-methods approach comprising desk research, surveys, interviews and workshops. The consultation aimed at systematically collecting and analysing the perspectives of all key stakeholders, including public authorities, the private sector, civil society, members of academia, experts and individual citizens, to inform the evaluation conclusions and the policy-making process.

2. Mapping of stakeholders

The consultation activities to evaluate ENISA and the ECCF were designed to ensure broad and balanced representation of all relevant stakeholders in the European cybersecurity landscape. Stakeholders were identified and mapped according to their institutional role, their involvement in cybersecurity policy and practice, and their relationship to ENISA and the ECCF. This mapping informed the design and targeting of surveys, interviews and workshops.

The main stakeholder categories included:

- **EU institutions and bodies:** this group comprised the European Commission, the European Parliament and decentralised agencies with responsibilities in cybersecurity policy, oversight and implementation. Their input focused on policy development, regulatory coherence and cross-border coordination.
- **National public authorities:** national cybersecurity agencies, competent ministries, regulators and other authorities responsible for implementing and enforcing cybersecurity policy were included. These stakeholders provided perspectives on national approaches, regulatory challenges and the practicalities of executing policy.
- **Industry and private sector organisations:** this category included companies involved in developing, providing or operating digital products and services, such as hardware manufacturers, software developers, cloud service providers and cybersecurity solution vendors. Their input was essential for understanding the impact of certification schemes and regulatory requirements on market stakeholders.
- **Industry associations and representative bodies:** associations representing the collective interests of businesses and industry sectors were engaged to reflect the perspectives of both large enterprises and SMEs. These organisations often acted as intermediaries, helping their members participate in the consultation process.
- **SMEs:** these were consulted both directly and through representative associations. Their feedback was important for assessing the proportionality and accessibility of the regulatory framework, given their specific resource constraints and operational realities.
- **Academic and research institutions:** universities, research centres and think tanks with expertise in cybersecurity, standardisation and policy evaluation contributed analytical and technical perspectives. Their involvement ensured a robust assessment of the strengths and limitations of the current framework.

- **Consumer and civil society organisations:** organisations advocating for consumer rights, privacy, digital security and broader societal interests were included to ensure that the public interest was reflected in the evaluation. Their contributions addressed issues such as transparency, user protection and the societal impact of cybersecurity measures.
- **International organisations and standardisation bodies:** relevant international entities and standardisation organisations were engaged to provide input on how well European initiatives were aligned with global standards and practices.
- **Individual citizens:** members of the public were invited to participate, particularly through the targeted survey, to capture user experiences, perceptions of cybersecurity risks and expectations regarding digital security and trust.

This mapping ensured that the consultation strategy was inclusive and balanced, avoiding overreliance on any single group. It also guided the development of survey instruments and interview protocols, ensuring that questions were tailored to the specific roles and expertise of each stakeholder category.

3. Consultation activities

Consultation activities were conducted to support the evaluation of ENISA and the ECCF. The objective was to collect robust and representative evidence from all relevant stakeholder groups, ensuring that the evaluation was informed by a wide range of perspectives and experiences.

The main consultation activities included:

- **Call for evidence:** a call for evidence was organised to collect feedback from a wider audience, including stakeholders not directly targeted by the survey or interviews. The call for evidence was open from 14 July to 16 September 2023 and received 41 contributions from a diverse range of stakeholders, including business associations, companies, public authorities, consumer organisations, NGOs and individual citizens. The targeted survey provided additional perspectives on the effectiveness, efficiency and impact of ENISA and the ECCF.
- **Survey:** a targeted survey was conducted using the EUSurvey platform. The survey was designed to involve all stakeholder groups, including those involved with ENISA and the ECCF. It included both closed and open questions, with filtering to ensure that it was relevant to different respondents. The survey was sent to 856 stakeholders and was also promoted by the European Commission, ENISA and relevant associations. The survey was open from 13 February to 5 March 2024, with extensions to maximise participation. In total, 209 responses were collected, covering a broad spectrum of stakeholder categories, such as national authorities, industry stakeholders, academic institutions, consumer organisations and EU institutions.
- **Interviews:** a structured interview programme was carried out to gather in-depth qualitative insights. The study team contacted 182 individuals and conducted 49 interviews for ENISA and 13 for the ECCF. Interviewees included ENISA staff and representatives of the European Commission, national authorities, industry, academia and international organisations. The interviews were designed to explore key evaluation questions in greater detail and to validate findings from other consultation activities.

- **Workshops:** two main workshops were held for collective discussion and validation of findings. The first was a SWOT and recommendations workshop, which brought together stakeholders from academia, ENISA, the European Commission and industry to discuss strengths, weaknesses, opportunities and threats related to ENISA and the ECCF. This workshop included interactive polling and breakout sessions to gather detailed feedback and suggestions for improvement. The second workshop focused on validating preliminary evaluation results and collecting recommendations for future improvements. Participants included representatives from the European Commission, Member States and other key stakeholder groups.

The overarching objective of these consultation activities was to ensure that the evaluation of ENISA and the ECCF was informed by stakeholder input. Each activity was designed to capture a specific type of evidence: desk research provided context and baseline data; the survey programme enabled quantitative analysis of stakeholder views; interviews offered qualitative depth and validation; and workshops allowed collective reflection and consensus-building. Together, these activities ensured that the evaluation reflected the experiences, needs and expectations of all relevant stakeholders in the European cybersecurity ecosystem.

4. Call for evidence

The call for evidence was conducted from 14 July to 16 September 2023 to collect stakeholder feedback on the impact, effectiveness and efficiency of ENISA's mandate and the ECCF. The consultation aimed to gather views from a broad range of stakeholders, particularly those involved in the EU cybersecurity certification process. In total, 41 responses were received from 13 EU Member States and two non-EU countries, with the majority of contributions coming from the private sector. Nearly half of the respondents were business associations (20), followed by companies and businesses (9), public authorities (4), consumer organisations (1), NGOs (1), research centres and standards associations (4), and individual citizens (2). Most respondents (85%) were based in the EU, with the remainder from the USA and the UK. Sectoral representation was also diverse, with significant input from digital service providers, digital infrastructure providers, manufacturing trade associations and generalist organisations.

The call for evidence sought to assess three main areas: the overall organisation and performance of ENISA, the functioning of the ECCF and feedback on specific certification schemes, particularly the Cloud Services Scheme (EUCS). Stakeholder feedback on ENISA was generally positive, with around 30% of respondents recognising ENISA as a leading centre of cybersecurity expertise in the EU. Particularly appreciated were its contributions to cyber resilience, incident response and the promotion of cooperation and best practice exchange. However, almost 22% of respondents said that ENISA's resources and capabilities needed to be distributed adequately and consistently, citing also challenges in recruiting qualified staff. Stakeholders recommended increasing cooperation with academic and research institutions to maintain specialised expertise.

A recurring theme in the feedback was the need for greater transparency and stakeholder involvement in ENISA's processes. Over 40% of respondents expressed concerns about insufficient engagement, particularly for smaller organisations and civil society representatives. Stakeholders called for more meaningful participation and improved communication, and for 'update only' meetings to be avoided. While it was highlighted that ENISA engaged with Member States through the national liaison officers network,

some respondents noted limited benefits from existing working groups due to organisational challenges.

Regarding the ECCF, stakeholders generally viewed EU cybersecurity certification as a useful and promising tool, but highlighted several areas for improvement. Delays in adopting certification schemes and the Union rolling work programme (URWP) were frequently mentioned as limiting the impact of the framework. Approximately 34% of respondents reported that they were insufficiently involved in developing certification schemes). A similar proportion (32%) highlighted a lack of transparency in ECCF procedures, including opaque decision-making, insufficient information sharing and changes to draft schemes without prior consultation. Stakeholders emphasised the importance of increasing transparency regarding the composition and functioning of ad hoc working groups, and of ensuring that members have access to draft schemes and are promptly informed of significant changes.

The mandatory nature of certification schemes was another area of debate. Of the 34% of respondents who raised this issue, the majority were opposed to mandatory requirements, citing concerns about increased costs and barriers to the internal market, particularly for SMEs. Those in favour of mandatory certification stressed the need for sectoral approaches, alignment with international standards and the use of impact assessments to evaluate the potential effects on economic operators and the internal market.

The Cloud Services Scheme attracted particular attention, with 9 out of 10 stakeholders concerned about the certification process being politicised, especially regarding data localisation requirements. Respondents warned that such requirements could disrupt business relationships and hinder market competition, particularly for providers headquartered outside the EU.

Stakeholders also stressed the importance of aligning EU certification schemes with international standards (21% of respondents) and ensuring coherence with the broader EU legislative framework (20%). Recommendations included streamlining compliance, allowing audit reports to be reused for multiple legal acts and ensuring mutual recognition of cybersecurity certificates across EU countries.

In summary, the call for evidence highlighted both strengths and areas for improvement in ENISA's mandate and in the ECCF. Stakeholders recognised ENISA's expertise and positive impact, but called for adequate resources that are distributed appropriately, for greater transparency and for more inclusive stakeholder engagement. As regards the ECCF, the feedback underscored the need for schemes to be adopted in a timely manner and for greater transparency, stronger stakeholder involvement and alignment with international standards and EU law. The consultation also revealed concerns about certification processes being politicised by considerations related to non-technical risk factors. Overall, the feedback emphasised the importance of collaborative and inclusive approaches to developing effective European cybersecurity policies and certification frameworks.

5. Targeted survey

The targeted survey formed a central part of the evaluation of ENISA and the ECCF. It aimed to collect evidence and perspectives from a broad pool of stakeholders across the European cybersecurity ecosystem. The consultation was designed to assess the effectiveness, efficiency, relevance, coherence and added value of ENISA and the ECCF,

and to ensure that the evaluation was informed by the experiences and expectations of all relevant stakeholders. This included stakeholders directly involved with ENISA and the ECCF, as well as those who benefit from their outputs and activities.

The survey programme was conducted via the EUSurvey platform, with the questionnaire developed on the basis of desk research, initial interviews and feedback. The survey included both closed and open questions, with filtering and branching logic to ensure that respondents were asked questions relevant to their background and involvement with ENISA and/or the ECCF. The survey was launched on 13 February and closed on 5 March 2024, with extensions and follow-up reminders to maximise participation.

5.1 Stakeholder participation

A total of 856 stakeholders received a personal invitation to complete the survey. The survey link was also promoted via the Commission's news page, in ENISA's internal communications and by the relevant associations. Up to three follow-up emails were sent to non-respondents and the deadline was extended by one week to accommodate additional responses. In total, 209 responses were received, representing a broad cross-section of stakeholder groups and ensuring a robust and representative evidence base for the evaluation.

Table 1. Number of survey responses per stakeholder group (overall)

	ENISA Ad hoc Working Groups	ENISA Advisory Group	ENISA Executive Board	ENISA Management Board	ENISA National Liaison Officer	ENISA Staff	External to ENISA	Total
Academia / research	2	2					3	7
Consumer organisation		1					4	5
EU institution/ body	2	3		1			7	13
Individuals	1	4						5
Industry organisation	23	21					18	62
International body or network		1					5	6
National cybersecurity authority/ agency	22		2	7	10		37	78
Other competent authority	5			1			13	19
Other		1						1
Total	**55**	**33**	**2**	**9**	**10**	**13**	**87**	**209**

ECCF-specific stakeholder participation

Of all the respondents, 70 (33%) indicated that they were involved with the ECCF and received a specific set of questions about its implementation. The breakdown for ECCF stakeholder groups is as follows:

Table 2. Number of survey responses per stakeholder group (ECCF)

Stakeholder group	Number of responses
ENISA ad hoc working group(s) related to cybersecurity certification	37
Stakeholder Cybersecurity Certification Group (SCCG)	24
European Cybersecurity Certification Group (ECCG)	21
National Cybersecurity Certification Authorities	19

Note: Respondents could select more than one option.

5.2 Summary of results

ENISA survey results

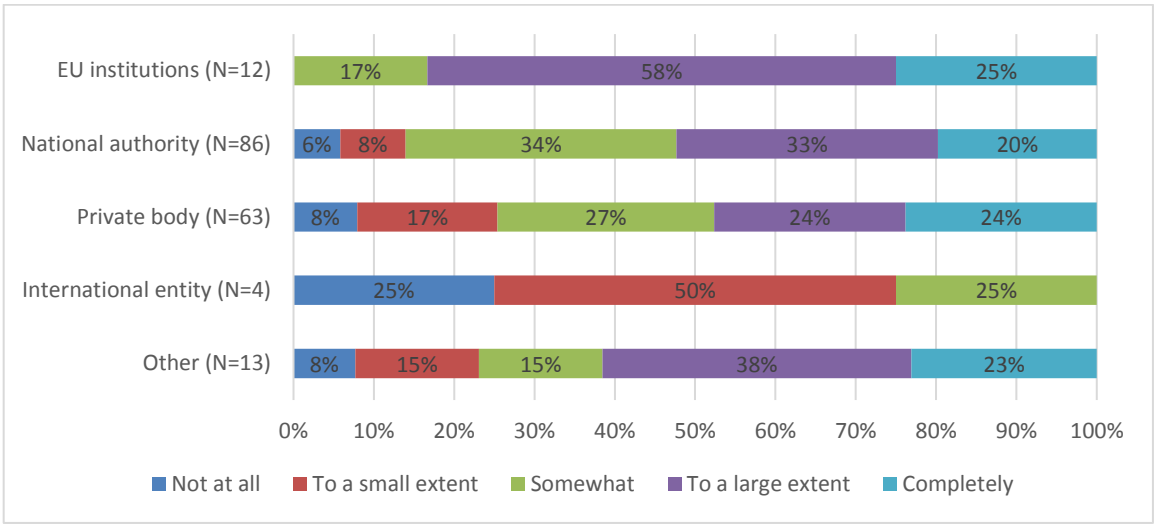
Effectiveness

ENISA is generally acknowledged by stakeholders as effective in fulfilling most of its mandate. According to the survey, 71% of stakeholders considered ENISA a leading centre of expertise on cybersecurity, able to deliver valuable outputs, including for policy-making and decision-making processes. ENISA's support was particularly appreciated during critical periods, such as the COVID-19 pandemic, and for its operational cooperation with Ukraine.

ENISA's publications were cited most frequently by stakeholders in the cybersecurity field, confirming ENISA's status as a centre of expertise in this area. Between 2017 and 2023, ENISA produced and issued a total of 286 publications. These covered a wide range of topics, with the most frequent being cybersecurity policy (72 publications), cyber threats (48), critical infrastructure (38), incident reporting (24) and emerging technologies (21). Stakeholders were involved in the preparation of these publications through workshops and studies. While these publications were highly cited and appreciated for their independence and clarity, many respondents noted in the open-ended follow-up questions that these could be made more concise and practical. There was a clear call for using summaries and visualisations more widely to make key information easier to identify.

Supporting policy implementation is one of ENISA's key tasks, as reinforced by the Cybersecurity Act. ENISA's support has contributed to its stakeholders adopting regulatory or policy changes and innovations. Respondents provided concrete examples, such as adopting structured threat communication protocols and using ENISA's guidance on implementing the NIS Directive to improve cybersecurity resilience. Respondents also underlined the influence of ENISA's frameworks on national cybersecurity certification schemes and the fact that ENISA's foresight activities helped anticipate future regulatory needs. Over 80% of ENISA's contribution was related to organising workshops and conferences. However, according to survey results, only about half of national authorities and companies consistently used ENISA's outputs for policy- or decision-making processes.

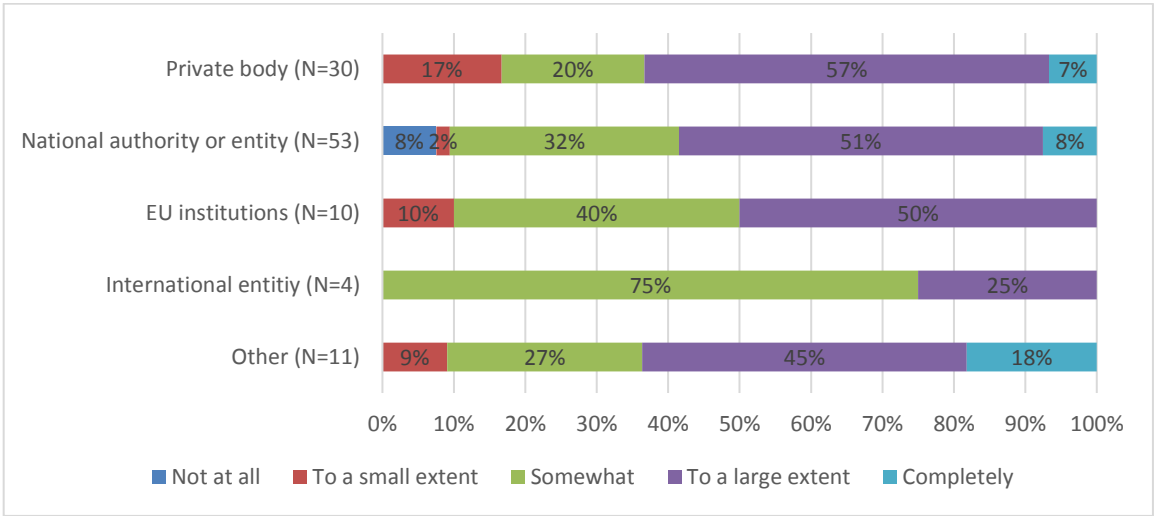
Figure 1 ENISA's outputs in policy tasks



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 21 'Please indicate to which extent ENISA's activities and outputs contributed to the following aspects? My organisation uses ENISA's outputs in its policy and or decision-making processes'.

The consultation results also show ENISA's effectiveness in supporting Member States through the Cybersecurity Support Action. 58 % of all stakeholders agreed that ENISA effectively supported Member States in preventing and responding to cyberattacks through that Action, with no notable differences between various stakeholder groups. However, the consultation also revealed that 44% of survey respondents were unable to assess the usefulness of the Action, indicating that the visibility of the Action needed to be improved.

Figure 2 The Cybersecurity Support Action's support to Member States in preventing and responding to cyber attacks



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 25 'In your opinion, to which extent has the ENISA Cybersecurity Support Action been effective in supporting EU member states in preventing and responding to cyberattacks?'

In summary, while stakeholder satisfaction with ENISA's approach and activities is generally positive, given its valuable outputs and role as a centre of expertise in cybersecurity, there are areas where its relevance can be significantly improved. ENISA's contributions to policy implementation and capacity building are appreciated by

stakeholders, although there are clear opportunities for improvement in communication, stakeholder engagement and resource allocation.

Efficiency

During the 2017-2023 evaluation period, stakeholders were enthusiastic about ENISA's performance, praising it for successfully delivering its outputs even during periods of high workload, and recognising its operations as mostly efficient under its existing governance structure. Despite this, the evaluation and survey highlighted several key areas where stakeholders found that ENISA still had room to become more efficient.

Responses to open-ended questions showed that some stakeholders were confused about ENISA's role within the EU's cybersecurity framework. Notably, 28% of the respondents surveyed were more restrained with regard to seeing ENISA as the centre of expertise on cybersecurity. They noted that the lack of a more effective communication system jeopardises ENISA's standing as the centre of expertise and that the complicated structure of ENISA's website prevented them from interacting properly with its outputs.

Interviews with ENISA's staff, stakeholder surveys and internal documentation indicated that ENISA struggled to keep pace with increasing demands and struggled to fill specialised positions, exacerbated by a global shortage of IT and cybersecurity specialists. This led to delays, reprioritisation of tasks and periods of high stress and workload. Periods of high workload for ENISA were often associated with adopting and implementing new policies or legal acts, with developing cybersecurity certification and with operational activities related to geopolitical developments. However, 63% of stakeholders gave a positive assessment of ENISA's performance ('successful' or 'very successful') during such periods. The survey results indicate that ENISA's organisational arrangements were relatively well adapted to managing periods of high workload. A total of 84% of stakeholders 'completely', to a 'large extent' or 'somewhat' agreed with this statement.

However, resources and resource allocation, operational inefficiencies and challenges stemming from the political and regulatory environment were identified as the main obstacles to ENISA's performance during periods of high workload. The 2022 Staff Satisfaction Survey shows that 64% of respondents experienced stress due to high workload.

In 2023, an average of 76% of staff reported working more than 40 hours per week monthly and in 2022, 4 FTEs resigned due to overwork and work over weekend. Some stakeholders noted that more resources and, to some extent, a more agile approach to deploying resources could be a way for ENISA to better adapt to evolving cybersecurity demands and to minimise delays. Other stakeholders thought that ENISA could increase its capacity to provide policy and technical support by being more selective with its engagements and refining its operational focus areas.

Stakeholders also noted that budget management presents opportunities for improvement. Despite significant budget growth from 2017 to 2023, resource constraints persisted. ENISA's budget grew unevenly, with notable increases in 2019 (over 46%), 2020 (30.5%) and 2022 (72.4% compared to 2021, due to the Cybersecurity Support Action). ENISA encountered a downward trend in balancing approved and committed appropriations between 2019 and 2022 due to delays in actions like the Cybersecurity Support Action. Reversing this trend and dedicating efforts towards managing administrative expenditure, including addressing procurement delays, could further improve internal efficiency.

In summary, ENISA demonstrated efficiency in implementing its tasks, supported by a revised governance structure. However, stakeholders underlined opportunities for ENISA to become more efficient by improving its communications and by making more resources available or allocating resources in a more strategic manner.

Relevance

ENISA's relevance within the cybersecurity domain is shown by its responsiveness to evolving stakeholder needs and its flexibility to adapt to the changing landscape. According to stakeholders, it has consistently demonstrated its ability to review and realign its areas of action in response to emerging developments. Thus, it continues to be a vital part of the EU's cybersecurity framework.

The results of the survey confirmed that ENISA's work was mostly relevant to stakeholders' needs. It regularly reviewed its areas of activity to respond to emerging needs and remained agile by setting up ad hoc working groups. Stakeholders expressed a high level of satisfaction with how ENISA responded to changes in the cybersecurity landscape, although some felt that it needed more tools to effectively address the growing cyber threats in Europe. National cybersecurity authorities and smaller Member States benefited from ENISA's capacity building initiatives and regulatory insights. However, stakeholders noted that ENISA could further increase its relevance in some areas. To do this, they suggested that it improve its support and increase its visibility among various sectors and stakeholders, especially SMEs, which often find it hard to meet cybersecurity requirements. Stakeholders also called for more sector-specific tools and resources, as well as insights and tools to tackle emerging threats.

The stakeholders surveyed reported being satisfied with ENISA's ability to adapt to the changing cybersecurity landscape. Specifically, 74% of respondents mostly or strongly agreed that ENISA quickly adapted to changes in the cybersecurity landscape in 2019-2023, and 70% mostly or strongly agreed that ENISA sufficiently addressed all major unforeseen cybersecurity incidents during that period. There were no notable differences between the responses of different stakeholder groups.

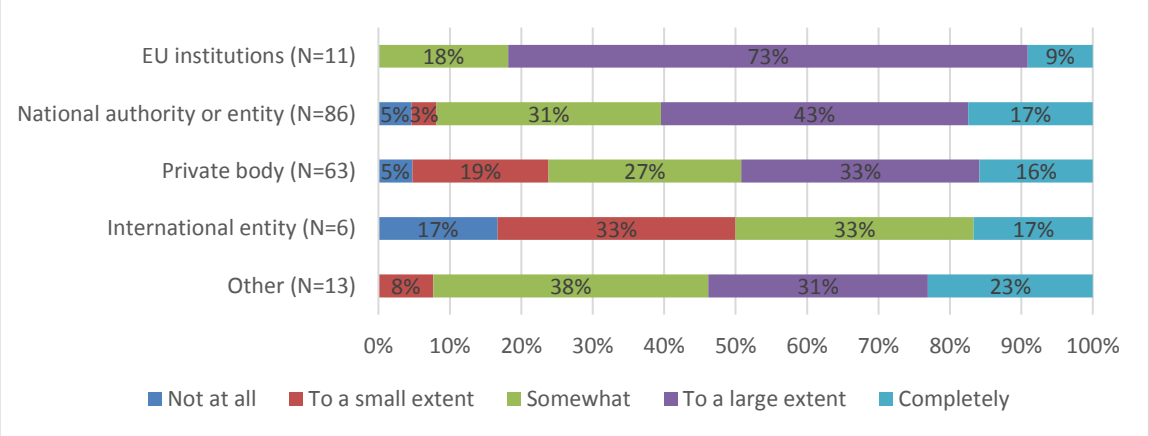
While stakeholders acknowledged ENISA's efforts, some respondents felt that it needed greater capabilities to effectively address all cyber threats in Europe. Respondents argued that ENISA lacked an effective incident response unit and operational capabilities to act quickly in the face of cybersecurity incidents. They felt that these were not sufficiently supported by ENISA's mandate and governance structure. Some respondents stressed that directly managing cybersecurity incidents was not the purpose of ENISA and that it had no capabilities in this area. Instead, ENISA supports Member States in dealing with incidents, and those respondents pointed to successes in this context with the CSIRTs network. ENISA contributed to the EU's preparedness to face cyber threats by supporting and organising cyber exercises and by improving operational cooperation between Member States, including through its support to the CSIRTs network.

ENISA set up appropriate practices for stakeholder consultation and management, however industry stakeholders expressed dissatisfaction with the consultation and collaboration processes that involved them, as well as with the difficulty in accessing information.

While ENISA's outputs and services generally align with stakeholder needs, notable discrepancies exist in how different groups of stakeholders perceive ENISA's responsiveness to their needs. ENISA's support is perceived as most relevant by EU

institutions, and relevant to a lesser extent by national authorities or entities and private bodies. The difference in the relevance of ENISA's work to its stakeholders was underlined by the varying level of satisfaction with its services and outputs. 44% of all respondents indicated that their needs were met only 'somewhat', 'to a small extent' or 'not at all'. This figure rises to 50% for respondents representing industry organisations, with a comparatively higher proportion of respondents selecting 'to a lesser extent'. This data suggests that there is still room for ENISA to tailor its efforts to better meet the needs of national organisations and private bodies.

Figure 3 Relevance of ENISA's support to different groups of stakeholders



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 21 'Please indicate to which extent ENISA's activities and outputs contributed to the following aspects: ENISA's outputs and services correspond to my organisation's needs'.

National cybersecurity authorities and agencies valued ENISA's role as a key facilitator of cooperation and information exchange between Member States, as well as in promoting technical cooperation and a common standard of cybersecurity. They also valued the insights provided by ENISA on new regulations, guidelines, best practices and national requirements. Capacity-building initiatives were particularly appreciated by smaller Member States with more limited internal capabilities, while support for common standards proved particularly beneficial for EU candidate countries.

Representatives of international organisations, industry and vendors highlighted the importance of ENISA in representing the EU's position in the increasingly complex regulatory landscape of cybersecurity compliance and technical policy. ENISA's role in facilitating cooperation between different types of national and international stakeholders was described as crucial for ensuring a common understanding among different stakeholders. However, respondents called for ENISA to play a more direct role in providing tools and support to different sectors in order to increase its visibility and impact. ENISA could improve support for SMEs across the Digital Single Market to help such companies better integrate and comply with cybersecurity standards.

ENISA's support to EU institutions was well received, including its support in promoting situational awareness and crisis management. Its role in collecting information and liaising with Member States on cybersecurity was also valued. Respondents from the Commission expressed confidence in ENISA as a reliable implementing partner and a source of technical and operational expertise. ENISA has made contributions to national and EU policies and legislative initiatives, which have been generally well received by stakeholders. According to ENISA, its ability to provide policy support to the Commission is mainly hindered by a lack of qualified policy experts.

The role and purpose of ENISA in policy-related tasks were found to be clear and properly defined, as confirmed by 72% of the stakeholders surveyed. However, some stakeholders had expected ENISA's role in policy-related tasks to go beyond its current mandate.

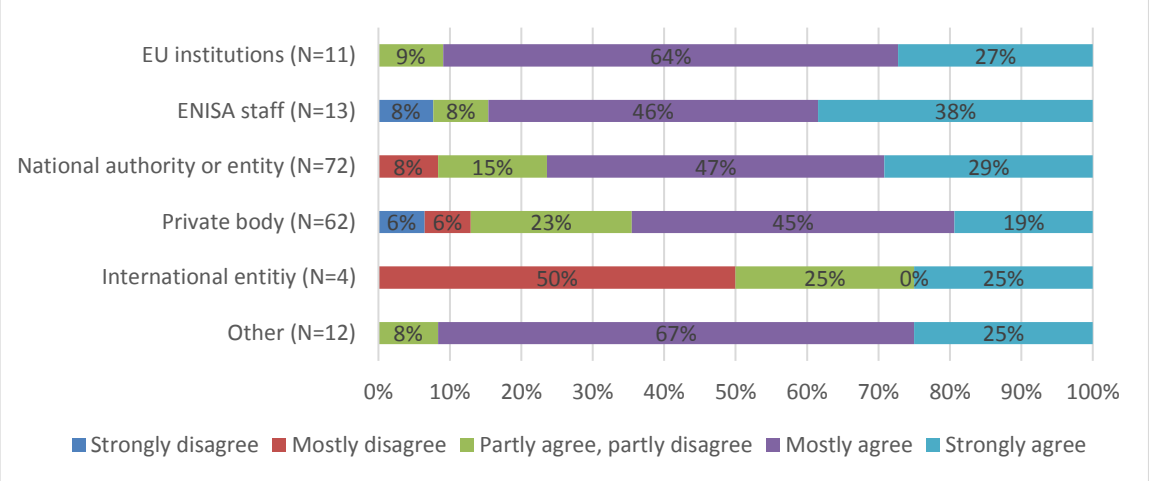
In summary, ENISA's relevance is well established, and its flexibility, strategic alignment and stakeholder engagement are valued. Nevertheless, stakeholders stressed that there is still significant room for ENISA to better meet their needs.

Coherence

ENISA played an active role in fostering cooperation and knowledge sharing among stakeholders, as confirmed by the results of the survey. Its efforts were thought to complement those of national cybersecurity authorities and CERT-EU, although some interviewees noted that there were areas of overlap. ENISA supported key EU networks such as CSIRTs and EU-CyCLONe, organised exercises such as CyberEurope, and facilitated the exchange of best practices through the NIS Cooperation Group.

Survey respondents provided a positive assessment of ENISA's efforts to exploit synergies in expertise and knowledge sharing with other stakeholders. Representatives of private bodies were somewhat less satisfied (65%) compared to other stakeholder groups (74% overall).

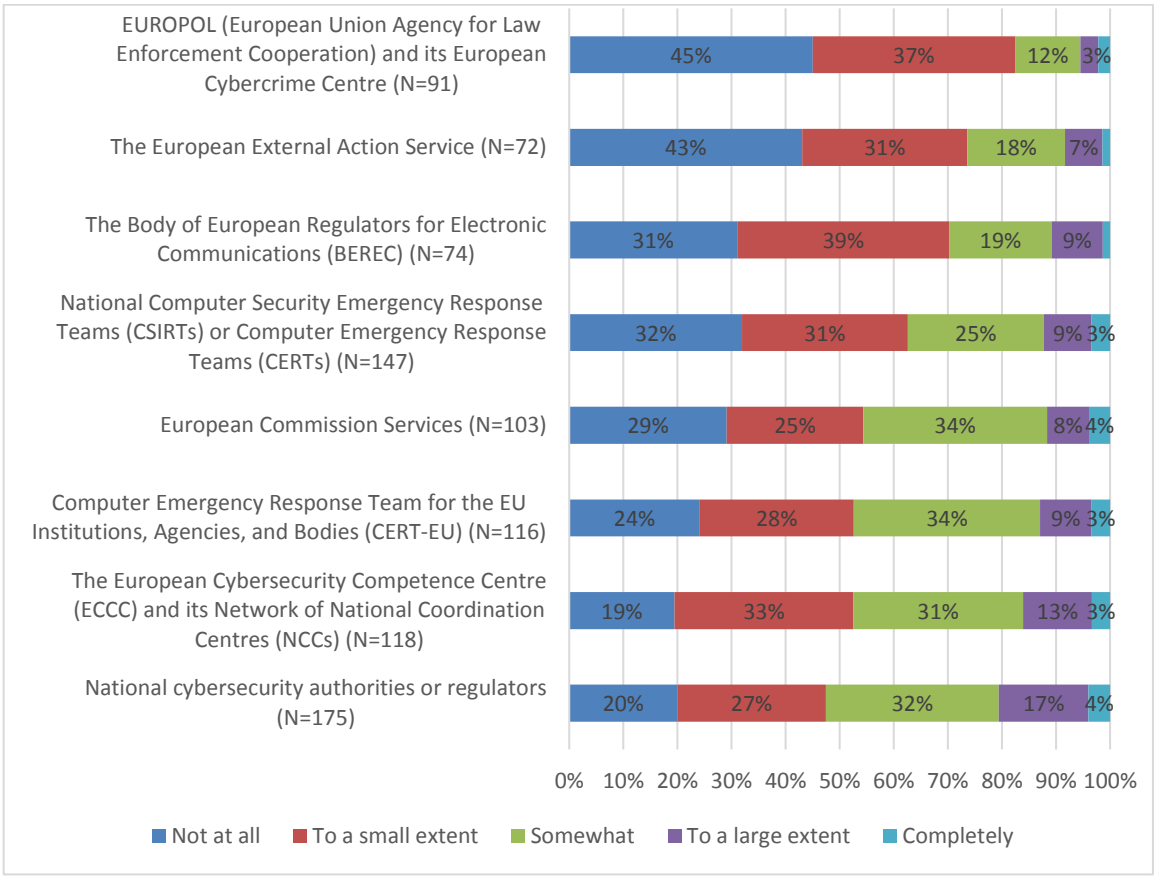
Figure 4 ENISA sufficiently exploited synergies with other stakeholders



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, questions 15 and 23: 'Please indicate to what extent you agree or disagree with the following statements about ENISA: ENISA sufficiently exploited synergies with other stakeholders'

There were a few overlaps between the formal responsibilities of ENISA and those of other relevant stakeholders, but these activities were mostly carried out in a complementary way. Stakeholders saw the greatest overlap between ENISA and the national cybersecurity authorities, the ECCC, CERT-EU and Commission services. They identified a need to improve synergies between the responsibilities and actions of ENISA and those of other EU bodies. Responses to open-ended follow-up questions indicated that there were already complementarities with national authorities in policy-related tasks, risk management, capacity building and incident response, which were mutually beneficial. Some survey respondents underlined that, by formalising cooperation arrangements with other entities, such as EMSA and the JRC, ENISA could better leverage synergies and ensure a unified approach to cybersecurity initiatives.

Figure 5 Overlaps between ENISA and other stakeholders in the field of cybersecurity

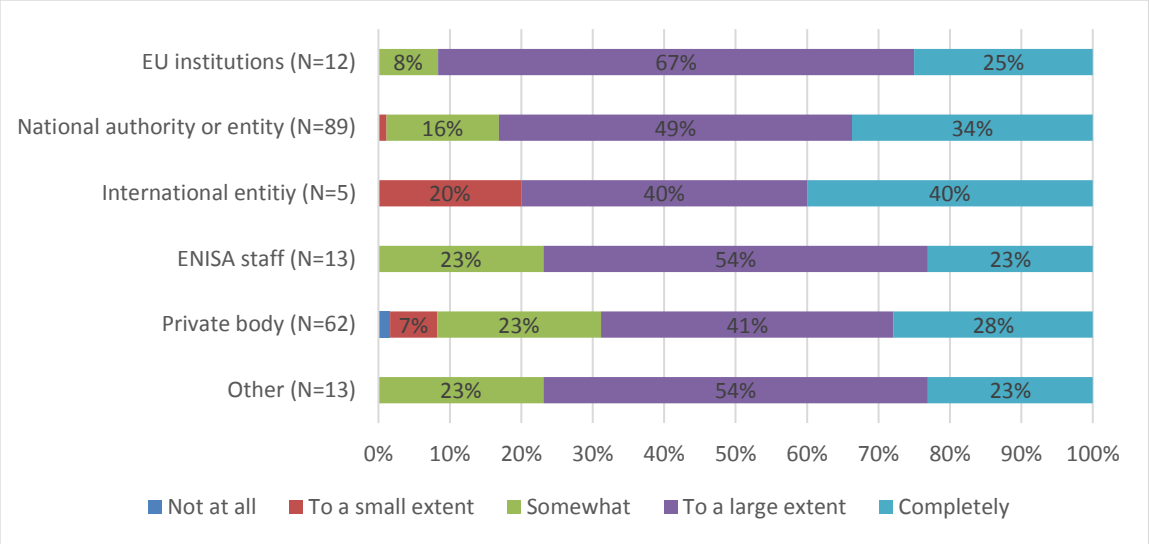


Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 26 'In your view, to what extent, if at all, do ENISA's outputs and services overlap with those of the following institutions active in the area of cybersecurity?'

ENISA strengthened its cooperation with EU, regional and international stakeholders during the evaluation period. This was demonstrated by the increasing number of structured cooperation frameworks set up. Several MoUs were signed with other EU bodies to improve working arrangements and facilitate the sharing of knowledge, information and expertise. ENISA also signed a service level agreement with the ECCC in the fields of research, innovation and administration in 2022. This was followed by an MoU in 2023 to coordinate the implementation of operational tasks and research initiatives. Despite this, some survey respondents still see a need to further calibrate activities and increase coordination between both organisations.

ENISA facilitated cybersecurity cooperation at EU and national levels. Stakeholders had positive opinions of ENISA's promotion of cybersecurity cooperation, including information sharing and coordination, during the evaluation period. National authorities assessed ENISA's contribution to cybersecurity promotion especially positively, with 83% of survey respondents indicating that it had achieved this objective to a large extent or completely.

Figure 6 ENISA's contribution to promoting cybersecurity cooperation

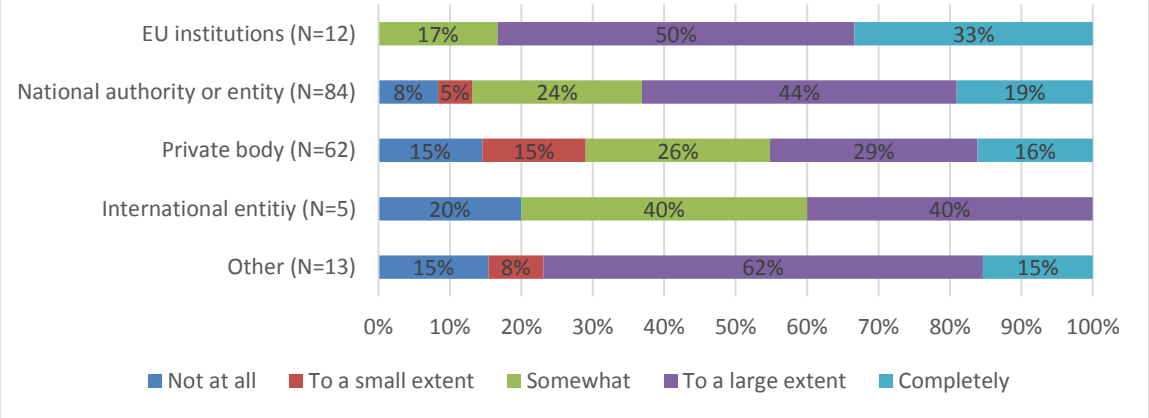


Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 16: 'In your opinion, to what extent has ENISA achieved the following objectives during the period of 2019-2023? Promoting cybersecurity cooperation, including information exchange and coordination, at EU level between MS, EU institutions, bodies, offices and agencies and relevant private and public stakeholders'

ENISA also strengthened its regional cooperation with non-EU countries, particularly with the Western Balkans and Ukraine. ENISA set up working arrangements with the US Cybersecurity and Infrastructure Security Agency (CISA) in the areas of capacity building, exchange of best practices and increasing situational awareness.

Survey respondents and interviewees expressed that ENISA's interactions with private stakeholders and international partners must be more predictable and transparent to maintain confidence and foster collaboration. Around half the representatives of private bodies found ENISA's role in contributing to cooperation and coordination between stakeholders to be limited. In this context, private bodies suggested that ENISA could improve its outreach and stakeholder engagement activities and could expand its partnerships with global cybersecurity stakeholders, particularly as regards collaborating with industry representatives and non-EU countries.

Figure 7 ENISA's contribution to cooperation and coordination between stakeholders



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 21 'Please indicate to which extent ENISA's activities and outputs contributed to the following aspects: The activities of ENISA have improved the cooperation and coordination between my organisation and other stakeholders'

In summary, stakeholders found that ENISA demonstrated a solid foundation in promoting cybersecurity coherence in the EU. They thought that its structured cooperation frameworks, support for key EU networks and facilitation of best practice exchanges contributed to a coordinated and coherent approach to cybersecurity across the EU. Some recommendations included addressing current inefficiencies and improving inter-Agency coordination.

EU Added Value

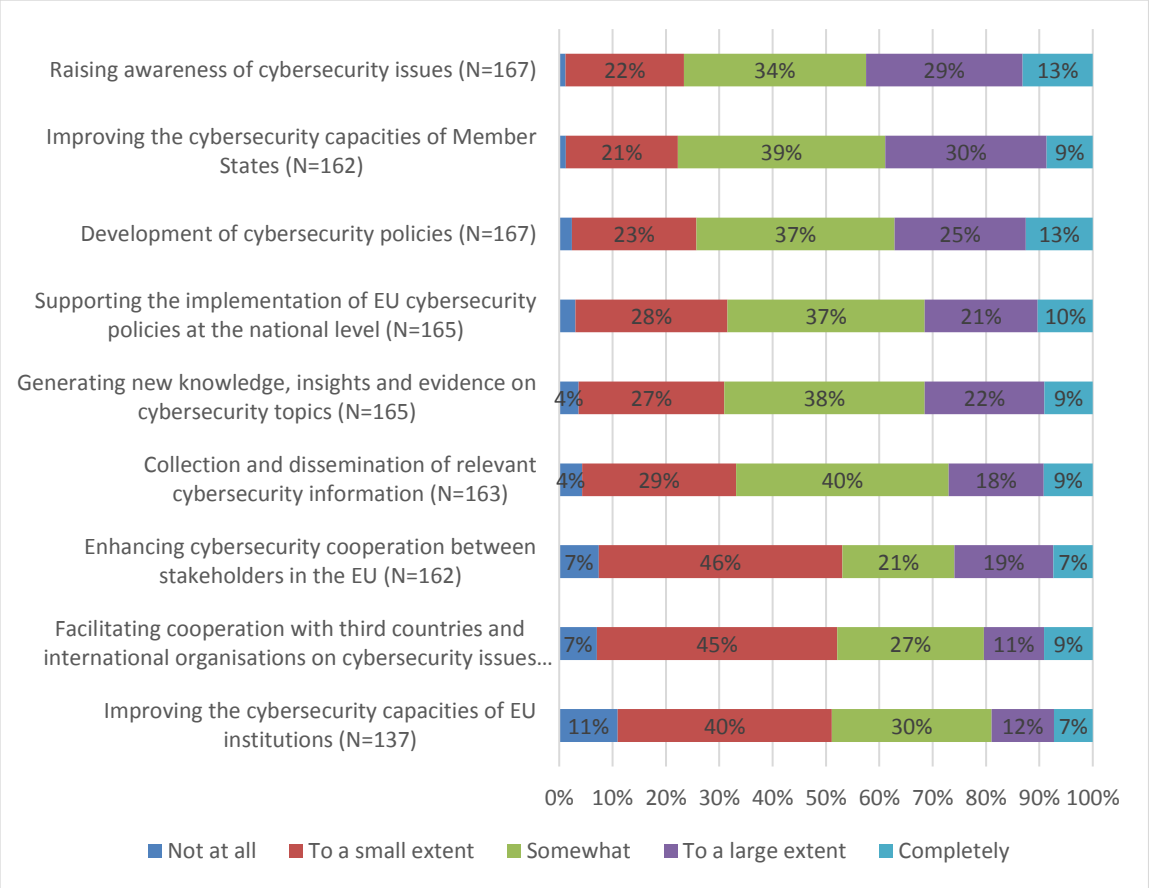
According to stakeholders and survey respondents, ENISA has made a significant contribution to the strengthening of the EU's cybersecurity ecosystem. It is seen as a central hub that has encouraged vital cooperation across the EU, supported national efforts, particularly in Member States with less mature cybersecurity frameworks, and helped align cybersecurity practices and policies. At the same time, stakeholders have identified areas where ENISA's impact could be reinforced.

ENISA's current configuration was considered optimal for maintaining independence and facilitating close cooperation with Member States. Stakeholders emphasised that ENISA's independence from political influence added great value.

ENISA's role in promoting convergence and harmonisation across the European cybersecurity landscape was achieved through active engagement with Member States, including the involvement of national experts in strategic and day-to-day discussions. ENISA coordinated with bodies such as CERT-EU, Europol and EC3 to produce joint reports, avoiding duplication and improving shared situational awareness. Agreements with other EU bodies, such as the ECCC and the European Union Agency for Railways (ERA), facilitated cooperation and avoided overlapping mandates. ENISA's secretariat roles in the CSIRTs network and EU-CyCLONe ensured continued coordination between and the effectiveness of these groups.

According to the survey, around two thirds of stakeholders considered that the collection and dissemination of relevant cybersecurity information, the generation of new knowledge, insights and evidence on cybersecurity issues and support for the implementation of EU cybersecurity policies at the national level would be hard to achieve without ENISA. Three quarters of respondents believed that improving Member States' cybersecurity capacities, and raising awareness of cybersecurity issues, would have little effect in the absence of ENISA. Around half of respondents believed that improving the cybersecurity capacities of EU institutions would be possible only to a small extent or would not be possible at all without ENISA. As for facilitating cooperation with third countries and international organisations, 45% of respondents said this would be possible only to a small extent without ENISA and 7% said it would not be possible at all. For enhancing cybersecurity cooperation between stakeholders in the EU, 46% said this would be possible only to a small extent and 7% said not at all.

Figure 8 Achieving ENISA's objectives without ENISA itself

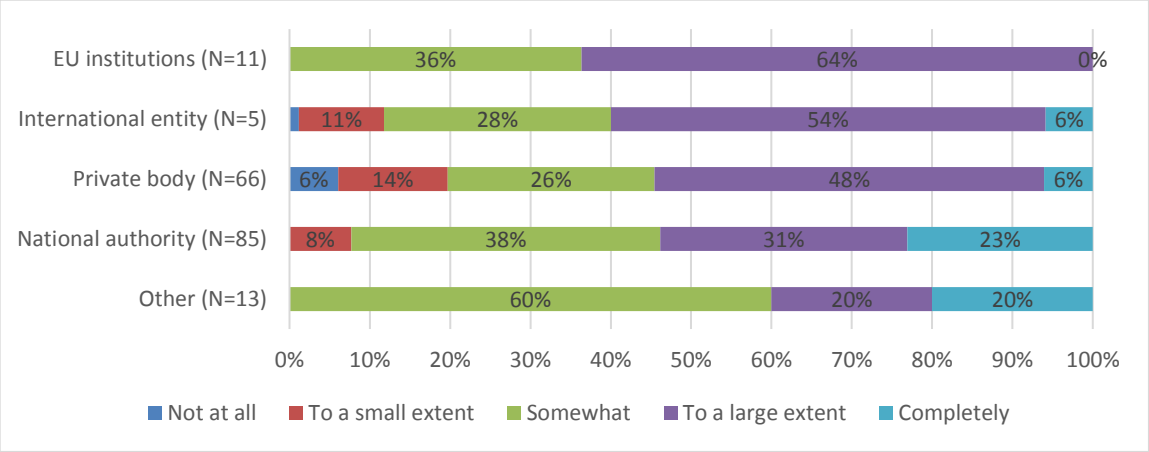


Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 34 'In your view, to what extent would the following results have been possible to achieve by Member States alone, without ENISA's involvement?'

Most respondents said ENISA provided clear EU-level added value to the cybersecurity of the EU. ENISA's specialised mandate, allowing it to act as a separate EU decentralised body, allowed for a dedicated and independent approach to cybersecurity. As an EU agency, ENISA's structure and governance allows for better and easier cooperation with Member States. Its expertise continues to be important in addressing the complex and evolving threats facing the EU.

However, private entities were more critical of the idea that ENISA provided added value. For example, 6% of private bodies responded 'not at all' and 14% 'to a small extent' when asked about ENISA's added value to their activities, compared to 0% and 8% respectively among national authorities. ENISA's primary focus was on national authorities, making sector-specific outputs less visible and impactful. The overall impact of guidelines and events depended on the level of maturity and specific needs of the organisation ENISA dealt with. Major industry players with a longstanding commitment to cybersecurity found ENISA's activities aligned with their routine operations but lacked new insights, indicating that more could be done to tailor insights to the private sector's specific challenges. Companies reported that they often relied on International Organization for Standardization (ISO)/ International Electrotechnical Commission (IEC) standards rather than ENISA initiatives. Some organisations valued ENISA's technical guidelines, tools and reports but claimed several of them were redundant in the context of existing standards. Private stakeholders monitored ENISA's work in areas such as IoT security and cybersecurity certification to ensure consistency with international standards.

Figure 9 Added value of ENISA's activities



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 35: 'Overall, to what extent has ENISA provided added value to the activities of your organisation during the period of 2019-2023?'

In the event of the withdrawal of EU action, the most likely consequences were expected to be increased difficulties in achieving trans-national coordination and the development of expertise in the field of cybersecurity. Overall, according to stakeholders, abolishing ENISA would lead to coordination challenges, less effective cybersecurity measures and potentially disjointed national approaches to cybersecurity issues.

ENISA is recognised for its specific focus on cybersecurity policy implementation, stakeholder engagement and comprehensive support to Member States, which positions it uniquely within the EU's cybersecurity landscape. While focusing on national authorities is essential, respondents said that ENISA could improve by increasing engagement with stakeholders and collaboration with industry. They also suggested that increased resources and better prioritisation could help ENISA adapt to evolving cybersecurity challenges.

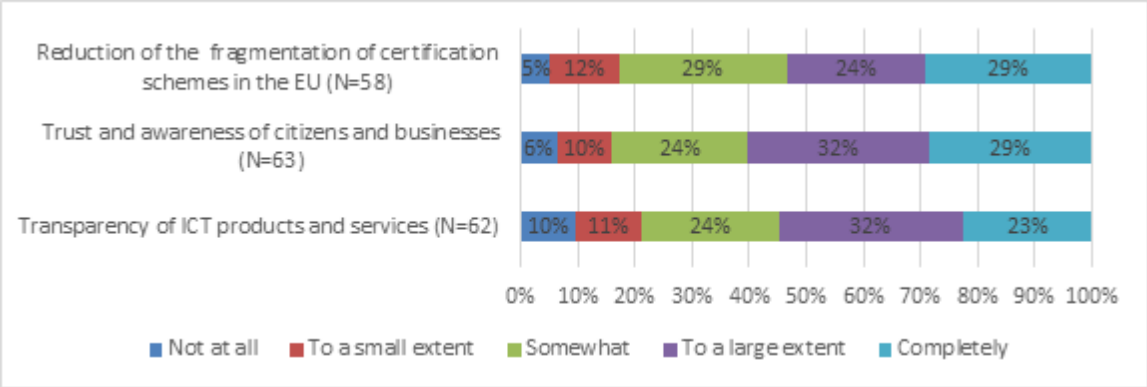
ECCF survey results

Effectiveness

The ECCF contributed only somewhat to improving the cybersecurity capabilities of Member States and private companies, according to the survey. 53% of stakeholders believed that the ECCF contributed only to a small extent to enhancing the capabilities and preparedness of private companies to face cybersecurity threats, while 19% did not consider the ECCF to have made any contribution to private companies at all. For Member States, 50% of survey respondents believed that the ECCF improved their capabilities only slightly, despite the establishment of national certification authorities across all Member States. The framework was considered to fall short in its ability to support national authorities in their efforts to increase national cybersecurity certification capabilities.

The survey results also indicated that delays in the adoption of certification schemes deeply affected the ECCF's ability to attain its objectives. Specifically, 55% of stakeholders believed that certification scheme delays negatively affected the ECCF's ability to improve the transparency of ICT products and services. Moreover, 61% said these delays negatively impacted the public's and businesses' trust in and awareness of cybersecurity, and 53% believed that delays hindered efforts to reduce the fragmentation of certification schemes within the EU.

Figure 10 Objectives that were not reached according to stakeholders

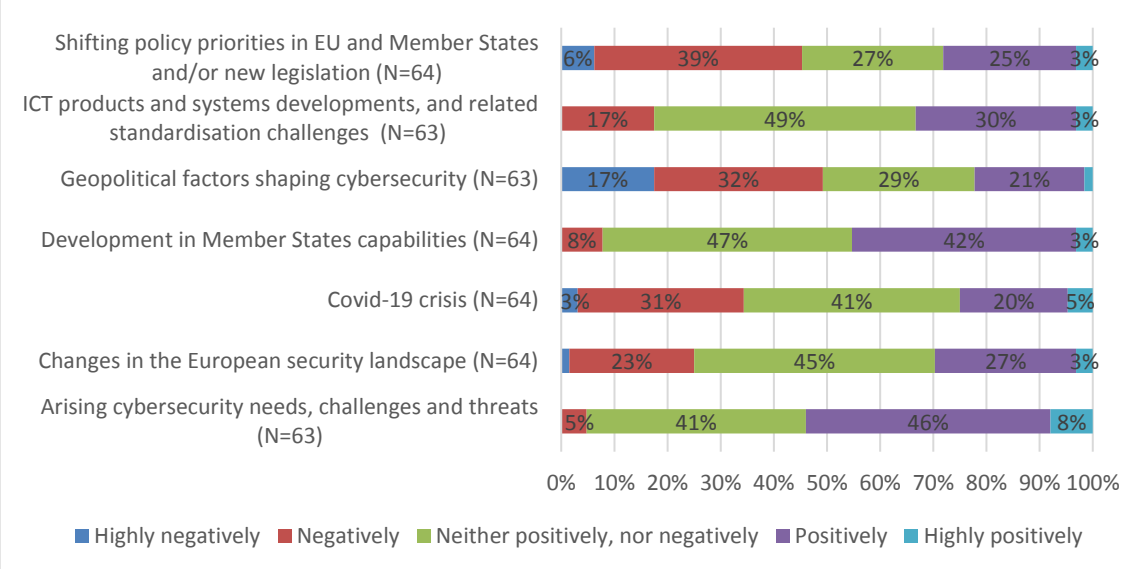


Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 48: 'Do you agree with the following statements'

Despite these challenges, according to the survey, 52% of respondents reported that the ECCF improved cooperation and coordination across Member States and EU institutions, bodies and agencies.

External factors also influenced the effectiveness of the ECCF. According to the survey, 46% of stakeholders said emerging cybersecurity needs, challenges and threats had positively influenced the ECCF's effectiveness; 42% of respondents indicated that the increase in Member States' capabilities in cybersecurity had had a positive impact on the ECCF. However, 45% of stakeholders considered that changes in policy priorities at the EU and Member State levels had had a negative impact on the ECCF. Geopolitical factors were also significant, with 49% of stakeholders saying that they had impacted the ECCF negatively or highly negatively. The COVID-19 pandemic had had a slightly negative impact, according to 31% of survey respondents.

Figure 11 External factors influencing the ECCF's objective



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 49: 'In your opinion, to what extent have the following external factors positively or negatively influenced the ECCF in achieving its objectives?'

In summary, the ECCF's effectiveness in fulfilling its objectives was limited by resource imbalances, delays in adopting schemes and external factors such as changing policy priorities and geopolitical influences. While the ECCF improved cooperation and

harmonisation among Member States and EU institutions, significant challenges remained in the drive to improve certification capabilities and reduce fragmentation across the EU.

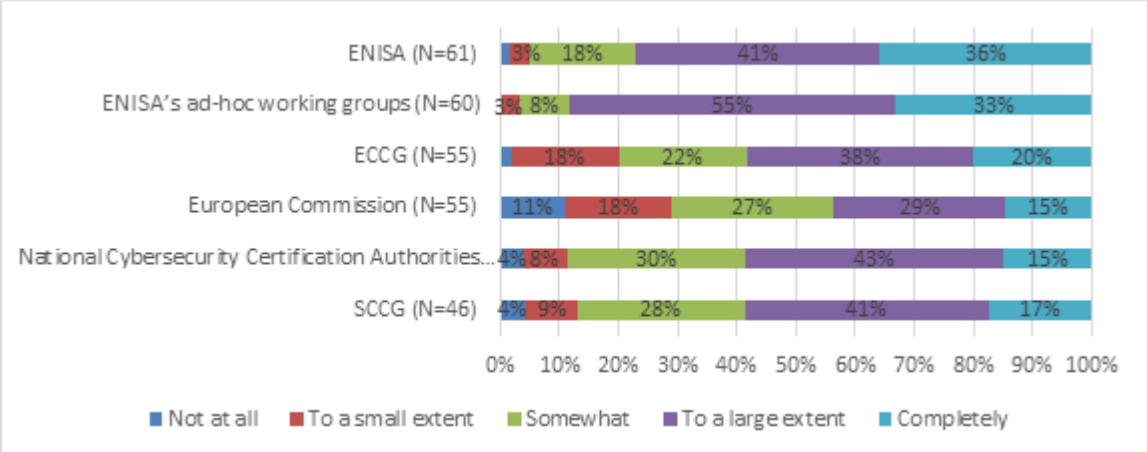
Efficiency

The efficiency of the ECCF was mostly impacted by content- and process-related issues. According to the survey, 77% of respondents reported that content issues, such as technical complexity or political impact, were the factor that most hindered the operation of the ECCF. 70% of respondents identified process-related issues, including the functioning of the preparation and adoption process, as significant obstacles to efficiency. Legal concerns, such as shortcomings in the legal framework at EU or national level, had less impact (identified by 43% of respondents).

As regards the EUCS scheme, 46% of survey respondents indicated that content issues, resulting largely from the politicisation of the debate, were the primary impediment to adoption. In the case of EU5G, 38% of stakeholders raised content-related issues and 32% attributed delays to process-related issues. The EUCC scheme was adopted in January 2024 after about 55 months of discussion, with delays attributed to technical complexity, lack of experience in developing schemes and changing policy priorities.

Survey respondents identified ENISA and its ad hoc working groups as the stakeholders that contributed most to the smooth functioning of the framework, with 77% and 88% of respondents respectively agreeing completely or to a large extent that these bodies had made a contribution. The ECCG, SCCG and NCCAs also garnered rather positive opinions, with 58% of respondents expressing a positive view for each of these stakeholder categories.

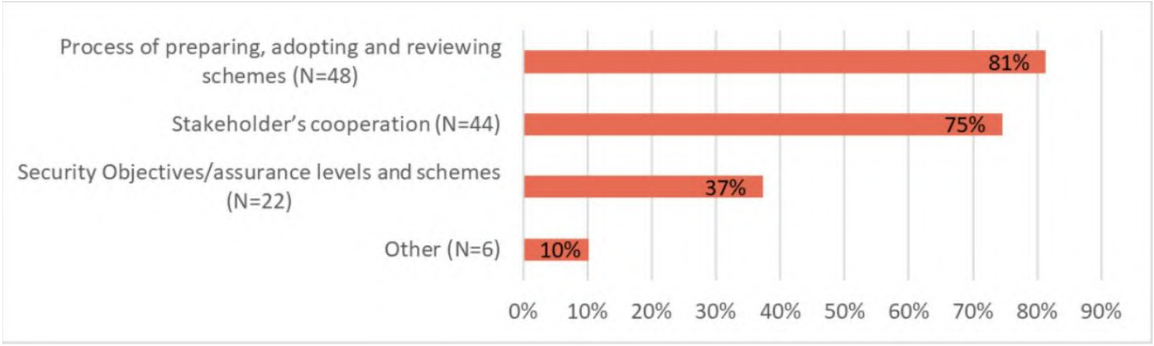
Figure 12 Stakeholders' contribution to ensuring smooth functioning of the ECCF



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 51: 'In your opinion, to what extent have the following stakeholders and processes contributed to ensuring a smooth functioning of the ECCF?'

According to the survey, areas of the ECCF that could be improved include the process of preparing, adopting and reviewing schemes (suggested by 81%), stakeholder's cooperation (75%) and security objectives/assurance levels and schemes (37%).

Figure 13 ECCF improvements



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 64: 'Which of the following areas of the ECCF, if any, could be improved?'

Given the EUCC scheme was adopted only recently, it is too early to identify the costs borne or the benefits experienced by stakeholders in terms of compliance with ECCF requirements. However, survey respondents indicated some costs and benefits related to preparatory activities, such as the development of standards, capacity building, and awareness-raising.

In summary, while ENISA and ad hoc working groups were seen as positive contributors, improvements are needed in the area of stakeholder cooperation and decision-making transparency, as well as in process management.

Relevance

The ECCF is seen as highly relevant to the achievement of internal market objectives in the current cybersecurity landscape. Stakeholders said that, given the increase in the number and intensity of cybersecurity threats, EU cybersecurity certification is a valuable asset. Key aspects that make ECCF relevant include the closer level of EU cooperation, its contribution to the development of standards and the ability to require critical infrastructures and public procurement beneficiaries to become certified. Stakeholders emphasised ECCF's capacity to effectively improve cooperation between EU Member States and to streamline trade by providing a unified certification platform.

The ECCF's relevance is further underscored by references to it in other EU legislation, including the Cyber Resilience Act (CRA), the NIS2 Directive and the European Digital Identity Regulation, which were all pending adoption by the co-legislators or proposed at the time of the evaluation. The CRA is expected to be crucial in promoting the certification of software and products with digital elements. The ECCF has provided input to the development of new standards and to addressing gaps in existing ones, such as for the cloud and 5G.

The mutual recognition of certified products, services and processes across the EU is still considered an effective tool to reduce individual costs for enterprises, thereby strengthening the single market and facilitating trade within the EU. The ECCF was also identified as a platform for cooperation among Member States at the EU level, aimed at fostering comprehensive evaluation and coordination.

Survey respondents confirmed the relevance of the ECCF's scope. Specifically, 86% agreed that the scope of the ECCF is sufficient in terms of the elements within each scheme

(security objectives, assurance levels and types of requirement) and 88% agreed that it is adequate to cover ICT products, processes and services.

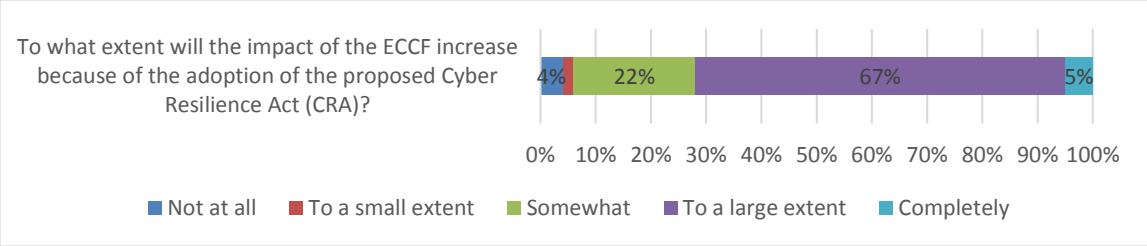
Coherence

The ECCF has demonstrated coherence with existing cybersecurity legislation and its operations are expected to be influenced significantly by the implementation of legislative measures such as the CRA, the European Digital Identity Regulation and the NIS2 Directive, according to the survey. Some stakeholders expressed concern about the risk of potential overlaps between the CSA and the CRA; this shows that real-world integration will be a challenge and will require oversight.

Ensuring the CSA's consistency with other EU policy and legislative measures, both cybersecurity-related (e.g. the NIS2 Directive and the CRA) and sectoral (e.g. the European Digital Identity Regulation), is essential for facilitating compliance and ensuring successful implementation of the ECCF. According to the survey, 83% of stakeholders found the framework to be coherent with existing instruments in the EU regulatory framework, with 55% answering 'fairly coherent,' 23% 'very coherent,' and 5% 'perfectly coherent.'

A broad majority – 72% of survey respondents – agreed that the then-planned adoption of the CRA would have a significant effect on the ECCF. The CRA is expected to introduce mandatory conformity assessment of cybersecurity requirements; existing certificates under an EU scheme may offer a presumption of conformity. While the CSA and CRA legal texts seemed fairly coherent, Member States stressed that it will be important to ensure a consistent implementation of the two acts.

Figure 14 Impact of the CRA proposal on the ECCF



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 63: 'In your view, to what extent will the impact of the ECCF increase because of the adoption of the proposed Cyber Resilience Act (CRA)?'

Despite recognising the overall coherence, more than half of respondents (54%) identified overlaps between the ECCF and other EU initiatives. Stakeholder contributions indicated that this concern stemmed from a potential overlap with the CRA, which could result in a duplication of efforts and inconsistent requirements. Member States also reported a risk of overlaps and noted the challenges involved in aligning the ECCF with international and European standardisation processes. They emphasised the need to establish a communication channel with international standardisation organisations to leverage existing European or international standards and prevent inconsistencies between standards developed at the EU and international levels.

In summary, stakeholders found the ECCF to be largely consistent with the existing EU regulatory framework, but also highlighted the importance of ensuring consistent alignment with forthcoming legislation and avoiding overlaps with other initiatives.

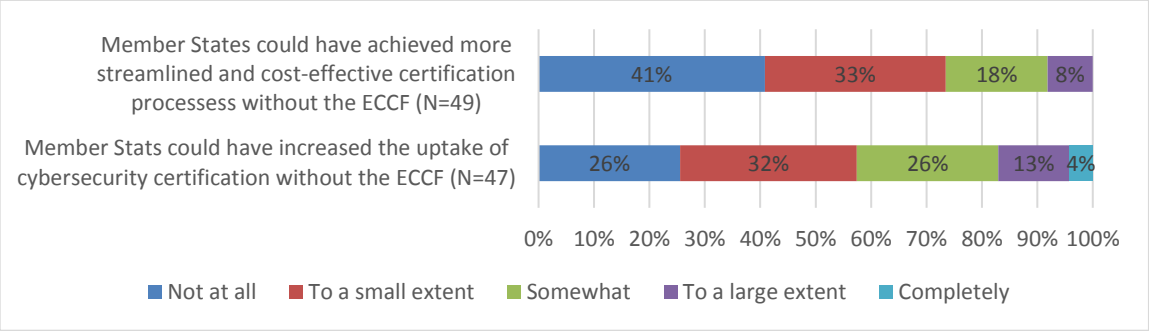
Continued attention to terminology and standardisation processes will be necessary to maintain coherence as the framework evolves.

EU Added Value

Stakeholders broadly agreed that the ECCF brings clear EU added value compared to what could have been achieved by Member States alone. The framework's harmonised approach to cybersecurity certification across all Member States provides a common EU baseline of security requirements for digital products, processes and services within the EU single market. This builds trust among consumers and businesses and promotes cross-border cooperation. Most stakeholders recognised the added value of the ECCF in achieving a more secure, transparent and cohesive internal market for ICT products, services and processes.

According to the survey, 84% of stakeholders believed that Member States alone could increase the uptake of certification only to some extent or to a limited extent. Furthermore, 92% of stakeholders believed that Member States alone could not have achieved more streamlined and cost-effective certification processes. For example, 41% of respondents said Member States could not have achieved more streamlined and cost-effective certification processes at all and 33% said they could have done so only to a small extent.

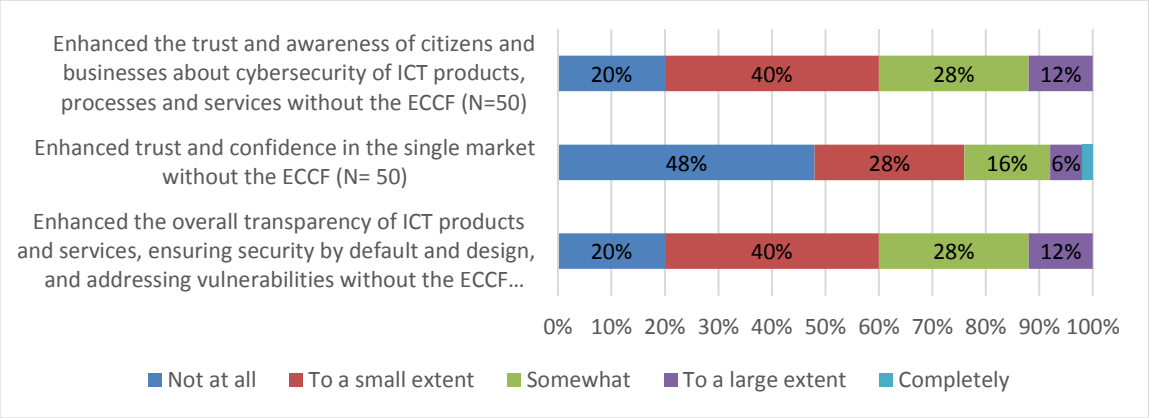
Figure 15 ECCF added value



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 60: 'Do you agree with the following statements?': 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have increased the uptake of cybersecurity certification more than what the ECCF has done' and 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have achieved more streamlined and cost-effective certification processes than what the ECCF has done.'

When considering the benefit of the ECCF on increasing levels of trust, 88% of stakeholders agreed that Member States alone might not be able, or able only in a limited way, to increase trust and awareness among the public and businesses about the cybersecurity of ICT products, processes and services. Additionally, 92% of stakeholders agreed that Member States alone could not have increased trust and confidence in the single market more than the ECCF had done. Regarding transparency challenges, 88% of stakeholders agreed that Member States alone could have increased the transparency of ICT products and services, ensuring security by default and design, only to a limited extent. For example, 48% of respondents said Member States could not have enhanced trust and confidence in the single market at all and 28% said they could have done so only to a small extent.

Figure 16 ECCF trust and transparency added value



Source: PPMI, Intellera Consulting and PwC (2024). Study to support the evaluation of the European Union Agency for Cybersecurity (ENISA) and the European Cybersecurity Certification Framework – Final Report. Survey of stakeholders, question 60: 'Do you agree with the following statements':' Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have enhanced the trust and awareness of citizens and businesses about cybersecurity of ICT products, processes and services more than what the ECCF has done', 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have enhanced trust and confidence in the single market more than what the ECCF has done' and 'Due to the delay in the adoption of European cybersecurity certification schemes, Member States alone could have enhanced the overall transparency of ICT products and services, ensuring security by default and design and addressing vulnerabilities more than what the ECCF has done.'

In summary, the ECCF's EU added value is widely recognised by stakeholders. The framework enables harmonised certification, increases trust and transparency and streamlines processes across the EU, achieving outcomes that would be difficult for Member States to accomplish on their own.

6. Targeted consultation (interviews)

As part of the evaluation of ENISA and the ECCF, a structured interview programme was implemented to collect qualitative insights from key stakeholders. In total, 49 interviews were conducted for ENISA and 13 interviews for the ECCF, involving a diverse range of participants including ENISA staff and representatives of the Commission, national cybersecurity authorities, industry associations and international organisations. The interviews were designed to complement the survey and the call for evidence by providing detailed perspectives on the implementation of ENISA's mandate, the functioning of the ECCF and the practical challenges and opportunities encountered by those directly involved in the European cybersecurity ecosystem.

ENISA

Interviewees consistently recognised ENISA's changing and increasingly central role in the EU cybersecurity landscape. ENISA was widely regarded as a trusted coordinator and facilitator, particularly valued for its support to Member States, its expertise in policy implementation and its contribution to operational cooperation. However, resource constraints were frequently mentioned as a limiting factor, with stakeholders noting that ENISA's expanding mandate and growing responsibilities were not always matched by adequate allocation or reallocation of financial and human resources. The agency's matrix-based organisational model and its governance structure were viewed positively, but interviewees called for further strengthening of internal coordination and prioritisation mechanisms to manage periods of high workload and to ensure the efficient delivery of outputs. Stakeholders from national authorities and EU institutions emphasised ENISA's valuable support in the implementation of cybersecurity policies, including the NIS Directive, the NIS2 Directive and sector-specific regulations. ENISA's technical guidance,

best practice-sharing and capacity-building initiatives were cited as particularly beneficial for smaller Member States and as being effective in harmonising approaches across the EU. However, some stakeholders expressed a need for more tailored, sector-specific guidance and for better dissemination of ENISA's outputs to ensure they are taken up in practice by a wider range of stakeholders.

The interviews highlighted ENISA's added value in fostering cooperation and knowledge-sharing among Member States, EU institutions and other stakeholders. The agency's role as a facilitator of networks such as the CSIRTs network and EU-CyCLONe was also appreciated. Nonetheless, several interviewees identified areas for improvement, including the need for more structured and regular engagement with industry, SMEs and civil society, as well as greater transparency and inclusiveness in stakeholder consultations. Some stakeholders suggested that ENISA could further strengthen its engagement with international partners and standardisation bodies to augment the global relevance of EU cybersecurity policies and certification schemes.

Across all interviews, there was a clear call for greater clarity, flexibility and resourcing at both the EU and national levels. Stakeholders recommended beefing up ENISA's mandate and resources to enable the agency to fulfil its expanding responsibilities, particularly in the areas of operational cooperation, policy support and certification scheme development. Suggestions included formalising ENISA's leadership in key networks, improving internal coordination and increasing the frequency and depth of stakeholder engagement. Interviewees also emphasised the need for ongoing investment in capacity building, knowledge-sharing and the development of sector-specific guidance.

ECCF

Interviewees provided detailed feedback on the implementation and governance of the ECCF. While the framework was recognised as a valuable tool for harmonising cybersecurity certification across the EU, stakeholders identified several challenges. Delays in the adoption of certification schemes, particularly the EUCC and EUCS, were attributed to complex technical requirements, political sensitivities and coordination difficulties among Member States and EU institutions. Industry representatives and national authorities expressed concerns about insufficient involvement in scheme development, limited transparency in decision-making processes and the need for clearer roles and responsibilities among key actors, including ENISA, the Commission and the ECCG and SCCG groups.

Interviewees also highlighted the importance of aligning certification schemes with international standards and ensuring consistency with other EU legislative instruments, such as the NIS2 Directive and the proposed CRA. The voluntary nature of schemes was not seen as a major problem, but the lack of experience in developing certification schemes contributed to delays and uncertainty. Stakeholders called for more structured engagement in the framework through clear processes and realistic timelines, as well as for regular meetings with clear objectives and sufficient time to prepare.

There was a strong emphasis on the need for more effective mechanisms to resolve political and technical deadlocks during scheme development, as well as for greater transparency and information-sharing throughout the process. Interviewees stressed that the ECCF's added value would only be fully realised if these governance and operational challenges were addressed, enabling the framework to deliver on its promise of a harmonised and effective European cybersecurity certification landscape.

7. SWOT and recommendations workshops

As part of the evaluation process for ENISA and the ECCF, two dedicated workshops were organised to facilitate collaborative analysis and gather targeted recommendations. These workshops brought together a wide range of stakeholders, including experts from academia and representatives from ENISA, DG CNECT, Member States and the study team. The workshops were conducted online and structured to maximise technical exchange, validation of findings and the formulation of actionable suggestions for future improvements.

7.1 SWOT Workshop

The SWOT workshop was held on 21 May 2024 via MS Teams, with 32 participants, including six study team members. The objective was to conduct an analysis of ENISA and the ECCF, using data collated by the study team and direct input from stakeholders. The workshop aimed to improve understanding of the strengths, weaknesses, opportunities and threats facing both ENISA and the ECCF and to foster dialogue on potential improvements to the Cybersecurity Act.

ENISA SWOT Results

Stakeholders confirmed the strengths identified by the study team, including ENISA's positive reputation within the EU cybersecurity community, the quality of its publications, effective collaboration among Member States, harmonisation efforts and capacity building. Its weaknesses were also attested, including resource shortages, strategic rigidity, potential delays, lack of clarity of ENISA's policy role and limited operational support. Opportunities identified included increased impact and services, collaborative training initiatives, the harmonisation of standards, policy engagement and an expanded mandate for more direct operational roles. Threats discussed included rapid technological advancement, the proliferation of funding initiatives, unexpected resource constraints, complacency and geopolitical instability.

ECCF SWOT Results

The ECCF SWOT analysis was similarly confirmed by participants. Strengths included boosting cooperation at EU level, adaptability to evolving technologies and legislative frameworks, the ability to mobilise experts and contribute to the development of standards, ENISA's capacity to ensure smooth scheme adoption, its relevance for internal market objectives and the added value of EU action. Weaknesses raised were the time-consuming scheme adoption processes, complexity in scheme development, susceptibility to geopolitical pressure and policy priority changes, a perceived lack of involvement of industry and external stakeholders and an unproven capacity to support cybersecurity preparedness and transparency.

Opportunities identified included greater flexibility and usefulness in tackling emerging threats such as artificial intelligence, strengthening Member State capabilities, the possibility of using certification as a presumption of conformity, potential mandatory requirements from upcoming legislation, the extension of its scope to managed security services, and providing impetus to standardisation processes. Threats included a lack of resources, potential shifts in policy priorities, increasing geopolitical instability, the risk of overlaps with other EU legislation and a risk of internal market distortions due to national cybersecurity requirements.

7.2 Recommendations Workshop

The recommendations workshop took place on 12 July 2024, also via MS Teams, with 77 participants, including seven study team members. The aim was to gather ideas for improving the performance of ENISA and the ECCF, drawing on the evaluation results and stakeholder input.

ENISA Recommendations

Polling results showed an average score of 3.9 (on a scale from 1 (not at all) to 5 (completely/fully agree)), indicating general agreement with the evaluation findings but with some reservations, particularly regarding efficiency and internal governance. Stakeholders emphasised the need for adequate financial resources and stressed the importance of maintaining a clear focus within the mandate to avoid resource dilution. Coordination with other bodies such as ECCC, EU-CyCLONe and CSIRT was highlighted as a way of avoiding duplication and improving efficiency.

Suggestions for governance included creating platforms for Member States to share information, streamlining the production of reports and balancing ENISA's advisory and executive roles. The importance of seconded members from Member States for increasing alignment with national priorities was noted, though retaining qualified staff remains a challenge. Stakeholder engagement should be efficient and tailored to different audiences, with feedback systematically incorporated into future planning.

ENISA's position in the EU cybersecurity landscape could be strengthened by it prioritising services and support to Member States, acting as an impartial facilitator and fostering robust cooperation with bodies such as the ECCC. Suggestions were also made for ENISA to establish cooperation with US entities such as MITRE[17] and NIST (regarding the NVD)[18] to improve threat intelligence and vulnerability management.

ECCF Recommendations

Polling results for the ECCF averaged 3.8 (on a scale from 1 to 5), indicating general agreement with the evaluation findings, but revealed more disparate views on coherence and added value. Discussions focused on the future purpose and scope of EU certification, with participants divided on whether the ECCF should address non-technical threats. Some argued for keeping the framework technical while others saw value in using certification to address strategic issues.

Process improvements were suggested across all stages of scheme development, including early preliminary assessments, realistic timeframes, increased involvement of the ECCG and early legal advice from the Commission. Greater independence for ENISA in scheme development and limiting political elements were also recommended. Simplifying administrative processes and considering the elimination of implementing acts for voluntary schemes were proposed to streamline adoption. Participants discussed the future roles of stakeholders, including the role of the ECCG in the maintenance of the schemes. Alignment with existing standardisation efforts was emphasised, as was the need for more industry involvement and input from independent experts.

[17] https://www.mitre.org/
[18] NVD - Home