Council of the European Union

Brussels, 21 January 2026
(OR. en)

5565/26

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.:	COM(2026) 9 final
Subject:	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 COM(2026) 9 final.

Encl.: COM(2026) 9 final

EUROPEAN
COMMISSION

Brussels, 20.1.2026
COM(2026) 9 final

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

{SWD(2026) 2 final}

1. INTRODUCTION

1.1 About ENISA

Established in 2004, the European Union Agency for Network and Information Security (ENISA) initially aimed to ensure a high level of network and information security within the EU and cultivate a security-conscious culture for the benefit of its stakeholders. Over the years, the Agency's mandate and responsibilities have significantly evolved to keep pace with the rapidly changing digital security landscape in Europe. In response to the increasing complexity of cybersecurity challenges, in 2019 the Cybersecurity Act (CSA) expanded ENISA's mandate and granted it permanent status within the EU institutional framework. This expansion of mandate further strengthened ENISA's role in supporting managing and coordinating cybersecurity efforts across the EU, focusing on several key areas:

- assisting the development and implementation of EU policy and law related to cybersecurity;
- enhancing the EU's capacity to prevent, detect and respond to cybersecurity incidents, particularly by providing operational and technical assistance to Member States and EU institutions;
- fostering cybersecurity capacity building and cooperation within the EU;
- raising awareness of cybersecurity risks and promoting best practices among the public, organisations and businesses;
- contributing to setting up and implementing the European cybersecurity certification framework, aimed at reducing market fragmentation and bolstering the cybersecurity of ICT products, services and processes across the EU; and
- supporting cooperation with international partners in alignment with EU external policies.

ENISA's activities now encompass baseline security recommendations, threat landscape reports, guidelines for standardisation, and studies on best practices in various domains. The Agency organises workshops, exercises and training programmes to enhance expertise among cybersecurity professionals and policymakers. Furthermore, ENISA plays a key role in responding to requests from the Commission and Member States, supporting certification tasks and providing tailored advice on cybersecurity policy development and implementation.

The expected impact of ENISA includes improving network and information security within the EU, enhancing trust in the Digital Single Market and promoting cybersecurity cooperation among key stakeholders in Europe. As Europe continues its digital transformation, ENISA's adaptive strategies ensure the security and resilience of the region's digital landscape, addressing challenges such as cybersecurity threats, geopolitical tensions and policy fragmentation among Member States.

1.2 About the European cybersecurity certification framework (ECCF)

The European cybersecurity certification framework (ECCF) was instituted under the CSA, with the primary aim of enhancing the cybersecurity landscape across the European Union. The ECCF is designed to create a unified and horizontal approach to cybersecurity certification across Member States, thereby reducing fragmentation within the internal market for ICT products, services and processes. By doing so, it underpins market trust, fosters the growth of the EU cybersecurity market and ensures robust cybersecurity resilience and capabilities. The framework addresses six core needs:

- promoting EU-wide market trust;
- improving cybersecurity measures and resilience;
- setting high standards of resilience in market offerings;

- enhancing cooperation among cybersecurity stakeholders;
- reducing certification burdens; and
- raising cybersecurity awareness among the European public and businesses.

Moreover, the ECCF seeks to increase transparency in cybersecurity assurance, promoting security by design and default, which entails vulnerability mitigation and adherence to specific security requirements.

To achieve these objectives, the ECCF is built on several key pillars, with the development of European cybersecurity certification schemes being central to these efforts. The framework emphasises comprehensive cybersecurity assurance and resilience across the EU through these schemes. The framework fosters community building to provide crucial stakeholder input and facilitate cooperation with, and between, the Member States. The CSA also mandates a public consultation of all relevant stakeholders by means of a formal, open, transparent and inclusive consultation process, and the formation of ad hoc advisory groups to gather diverse perspectives and expertise as part of the certification scheme development process. ENISA is pivotal in orchestrating these efforts by systematically consulting stakeholders to ensure all legislative elements are addressed before advancing final candidate schemes to the European Commission for adoption.

The cybersecurity circumstances underpinning the ECCF's creation reflect a rapidly shifting threat landscape marked by increased occurrences of cyberattacks exploiting vulnerabilities and insufficient security practices, combined with the emerging fragmentation of certification in the EU. This landscape underscores the need for the ECCF's mission to ensure the integrity, confidentiality and availability of data throughout the lifecycle of ICT products, services and processes. Upon completion of its core activities, the ECCF is expected to produce several outputs, including scheme-related documents, publications, events and structural enhancements supporting implementation. These efforts aim to foster a higher uptake of cybersecurity certifications, streamline processes, increase internal market confidence and fortify both public and private sector capabilities.

Looking forward, the ECCF's contributions are expected to bolster the cyber resilience and competitiveness of the EU, assuring secure and seamless digital interactions within the EU while addressing emergent cybersecurity challenges. Major impacts are anticipated in the medium to long term, with favourable outcomes contingent on dynamic internal and external factors, including geopolitical shifts, evolving security landscapes and emerging market needs.

1.3 Purpose of the Report

This report aims to evaluate the impact and effectiveness of ENISA and the ECCF, considering the evolving technological and regulatory landscape. Following Article 67 of Regulation (EU) 2019/881, known as the Cybersecurity Act (CSA), this evaluation not only reviews ENISA's mandate and activities but also assesses the ECCF's role in fostering a secure cyber environment across the EU by 28 June 2024. The findings presented are drawn from the preparatory evaluation report completed in December 2024.

The analysis covers the period from 2017 to 2023 and serves several key purposes. Primarily, it seeks to scrutinise the performance, governance and working practices of ENISA and the ECCF. This involves determining the degree to which they have met their objectives and contributed to enhanced cybersecurity and internal market function within the EU. The evaluation focuses on five main criteria – effectiveness, efficiency, relevance, coherence and EU added value – thereby providing a framework to understand both entities' achievements and areas for improvement.

By examining these elements, the report offers insights into potential adjustments to ENISA's mandate and strategies for strengthening the ECCF's impact. Ultimately, these evaluations aim to facilitate informed decision-making to advance EU cybersecurity resilience. The report is structured into distinct sections: an introduction of ENISA and ECCF, an analysis of the evaluation findings and a synthesis of conclusions and recommendations.

Regulation (EU) 2024/2847 (the Cyber Resilience Act) introduces horizontal cybersecurity requirements for products with digital elements (hardware and software, including their components when placed on the market separately). It conditions their placement on the Union market to compliance with a set of essential cybersecurity requirements, following the approach of the Union's New Legislative Framework. The Cyber Resilience Act entered into force on 10 December 2024 and will apply in its entirety from 11 December 2027. The Commission's proposal was accompanied by a comprehensive impact assessment analysing the rationale behind the introduction of such rules. In light of this, and the fact that the CRA is still in its transition period, it was not deemed necessary to assess further in this report the third element referred to in article 67(3) CSA: "The evaluation shall assess whether essential cybersecurity requirements for access to the internal market are necessary in order to prevent ICT products, ICT services, ICT processes and managed security services which do not meet basic cybersecurity requirements from entering the internal market".

As the findings of this report underpin the policy aims of the CSA revision, this report accompanies the legislative act and therefore it is essential to be presented it as part of this package.

2. MAIN FINDINGS OF THE EVALUATION

2.1 ENISA

This section outlines the main findings of the evaluation of ENISA, focusing on its effectiveness, efficiency, relevance, coherence and the added value it brings to the EU cybersecurity landscape. Additionally, a closer examination of the internal governance and practices within the Agency is provided to shed light on its operational dynamics and areas for improvement.

Effectiveness

The preparatory evaluation report highlights that ENISA has fulfilled its mandate by delivering nearly all planned outputs. It has to be mentioned though that with no sufficient indicators in place, the effectiveness analysis is based mainly on the interviews and surveys of the stakeholders. Notably, during challenging times such as the COVID-19 pandemic and Russia's war of aggression against Ukraine, the Agency demonstrated flexibility and achieved positive evaluations from stakeholders. During the COVID-19 pandemic, ENISA supported the Commission and Member States by defining security requirements for the COVID application at short notice. It also played a role in cooperation with Ukraine that aimed at ensuring that there were no spill-over effects of attacks on critical infrastructure and sectors such as energy. ENISA's effectiveness stems from a robust governance structure and a matrix-based organisational model that facilitates task delivery and cooperation. ENISA has achieved many of its objectives. Stakeholders generally recognised and appreciated ENISA's contributions to enhancing the EU's cybersecurity resilience. The Agency promoted cooperation and information exchange among Member States and other stakeholders to support the EU's cybersecurity objectives. The Agency's efforts in facilitating technical cooperation, promoting common cybersecurity standards, and supporting capacity-building initiatives were particularly valued. . The evaluation report also suggests that there is

room to improve task prioritisation in ENISA's ways of working. 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 the Agency's operational capacity shows insufficient resources. A use of a more dynamic reallocation of tasks and resources could partially help in ensuring timely fulfilment of new requests and enhancing ENISA's ability to respond to cybersecurity challenges to a certain extent. The Agency's aim to maintain and bolster 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. Such prioritisation should be facilitated through collaborative efforts between ENISA, Member States and EU policymakers to ensure alignment with strategic objectives and operational capacity.

Efficiency

During the evaluation period 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. However, there is a clear opportunity for ENISA to enhance its efficiency through improved prioritisation, clear focus and more strategic resource allocation. The Agency'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.

Despite this, the evaluation highlighted several key areas where ENISA has room to improve its efficiency. Interviews with ENISA's staff, stakeholders' surveys and internal documentation indicated that the Agency struggled to keep pace with increasing demands and to fill specialised positions, which was exacerbated by a global shortage of IT specialists. This has led to delays, reprioritisation of tasks, and periods of high stress and workload. Nevertheless, certain adjustments could alleviate these challenges. The recent strategic decisions to reallocate human resources demonstrate a capacity that can to a certain extent address priority shifts. Although a major budget increase of EUR 15 million has been implemented in 2022 to accommodate the Cybersecurity Support Action, this increase has not been matched by a proportional increase in staff. In fact, a reallocation of approximately 10.5 FTEs in 2022 to accommodate the Cybersecurity Support Action shows the ability to optimise current resources when necessary even though, in that case, the FTEs needed for implementing the Support Action were in fact obtained partially through procurement and partially through contract management staff, as highlighted in the preparatory evaluation report. The 10.5 FTEs were reallocated from the Agency's existing work programme, with 4 FTEs from Activity 4 ("Enabling operational cooperation"), 4 FTEs from Activity 5 ("Cooperative response at Union and Member States level"), and 2.5 FTEs from other activities. Consequently, ENISA took steps to deprioritise and/or scale back certain activities in 2023, shifted its human resources towards operational tasks deriving in particular from concrete tasks in legislation, with negative side effects for other tasks which were less clear from the ENISA mandate, e.g. on skills and awareness.

Budget management also presents opportunities for improvement. The Agency encountered a downward trend in balancing approved and committed appropriations between 2019 and 2022 due to delays in actions like the Cybersecurity Support Action. By reversing this trend and dedicating efforts toward

managing administrative expenditure, including addressing procurement delays, internal efficiency could see certain further enhancement.

Relevance

ENISA's relevance within the cybersecurity domain is underscored by its responsiveness to evolving stakeholder needs and its flexibility to adapt to the changing landscape. The Agency 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. While stakeholder satisfaction with ENISA's efforts is generally positive, there are dimensions where its relevance can be further increased. Despite its responsive nature, ENISA could improve support and increase visibility among different sectors and stakeholders, particularly for SMEs, which often struggle to meet cybersecurity requirements. A shift towards providing more direct tools and resources that are tailored to specific sectors but also provide insights and tools to address emerging threats can increase the Agency's impact. The Agency'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. The Agency's ongoing initiatives, including developing cybersecurity guidelines and capacity-building programmes, reflect its commitment to fostering cooperation and reinforcing the EU's collective cybersecurity posture. Advocating for stronger collaboration across industries and improving information access could address some limitations perceived by the industry sector. ENISA's considerable potential to improve lies in re-evaluating priorities, streamlining processes and acquire new appropriate and maximising existing resources efficiently, thus reinforcing its foundational role in Europe's cybersecurity ecosystem. Through strategic alignment with the European cybersecurity strategy, ENISA's revisited priorities could create pathways for more impactful contributions. Enhancing the Agency's capacity to provide policy and technical support might involve providing for more resources and by being more selective with its engagements and refining its operational focus areas. In conclusion, while ENISA's relevance is clear, there is still room for improvement. By reprioritising activities and providing for more and optimising existing resources, ENISA can bolster both its efficiency and overall impact, aligning more closely with the dynamic requirements of the European cybersecurity landscape.

Coherence

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. 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 those of 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. The Agency's interaction with private stakeholders and international partners must be more predictable and transparent to maintain confidence and foster collaborative efforts. In alignment with the Cyber Resilience Act

(CRA) and NIS2 Directive, a clear delineation of ENISA's tasks in policy implementation support could enhance 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 a margin for the Agency to reprioritise its efforts. This approach will help it to fulfil its mandate efficiently and to 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.

EU Added Value

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, complemented national efforts, especially in Member States with less developed cybersecurity infrastructures, and aligned cybersecurity practices and policies. 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 focus on Member States is essential, given its role in providing insights into emerging threats and recommending tools and strategies for addressing them. The Agency could further strengthen international cooperation, in line with Union priorities, including with partners in third countries, international organisations and cybersecurity agencies, to better address the global nature of cyber threats. 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. Despite the absence of similar bodies with ENISA's expertise and organisational agility, 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. Though the primary focus on national authorities is crucial, strategically enhancing stakeholder engagement and industry collaboration could address these concerns. Additionally, ENISA's mandate could benefit from strategically reassessing its re priorities to adapt smoothly 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 contributing to 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 presents limited agility in responding to evolving cybersecurity threats, which may lead to potential delays in its activities. To mitigate challenges related to resource constraints, the consulted stakeholders[2] emphasised, among other things, the need for improved recruitment processes and workload management strategies. Expanding ENISA's mandate to enhance 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 contribution to policymaking processes.

Finally, ENISA's stakeholder consultation and management systems are deemed effective in facilitating management of stakeholder needs and expectations, yet a stronger, more transparent relationship with Member States is necessary to enhance 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 numbers.

2.2 ECCF

This section outlines the main findings of the evaluation regarding the ECCF, focusing on its effectiveness, efficiency, relevance, coherence and the added value it brings to the EU cybersecurity landscape. Additionally, it summarises the main identified strengths and weaknesses of the framework based on a SWOT analysis.

Effectiveness

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 was set up to tackle persistent issues such as market fragmentation and the need for enhanced transparency and greater public trust in digital solutions. Through its structured governance model involving entities like ENISA, European cybersecurity certification group (ECCG) and the Network of National Cybersecurity Certification Authorities, the ECCF 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 despite the framework's intention to harmonise certification processes, leading to inconsistency and inefficiency in cybersecurity assurance. This can be observed in the substantial delay in operationalising the first certification scheme, the EU common criteria (EUCC), which took 57 months from initiation to adoption. This delay highlights inefficiency within the framework's processes, predominantly influenced by the complex and multifaceted approval procedures. Moreover, ambiguity in responsibilities and accountability among stakeholders has further complicated the framework's ability to achieve its objectives. 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 (European cloud certification scheme), 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 underscored the necessity for resilient digital infrastructure, thrusting cybersecurity into the policy spotlight. The COVID-19 had both negative and positive influences on the ECCF. On the 'negative' side, the sudden transition to online meetings contributed to delayed scheme development processes. On the 'positive' side, the COVID-19 pandemic raised awareness regarding the importance of resilient supply chains that are less reliant on third countries. Additionally, the analysis identified key lessons, noting the uneven resource allocation across stakeholders including Member States, which hinders the uniform development and implementation of

certification schemes. 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.

Efficiency

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

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 EU cloud certification scheme (EUCS) was impacted significantly by debates around data sovereignty requirements, drawing political pressures from third countries and industry outside the EU, leading to shifts from technical to political discourse within the ECCG.

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, requiring numerous stakeholders to ensure alignment with existing policies and practices in many phases. Despite these cases of inefficiency, several positive elements arose within the framework. The creation of dedicated groups and forums, including the European cybersecurity certification group (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; for example, the SCCG members perceived a lack of involvement of the group in the ECCF. Refining internal governance is crucial to address the active participation and strategic input of stakeholders.

Relevance

The ECCF emerges as a crucial response to the growing complexity and sophistication of cyber threats across the EU, aspiring to establish harmonised cybersecurity certification schemes that assure 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. This delayed fruition of tangible results underscores disparities in execution and casts uncertainty over the ECCF's current standing in the cybersecurity landscape. 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 enhancing the functioning of the internal market. The framework seeks robust integration with other EU legal acts, aiming to streamline procedures and facilitate cross-border trade.

Several factors bolster the ECCF's relevance despite the challenges it faces in carrying out its tasks. The surge in cyber threats greatly increases the need for a united cybersecurity strategy that can adapt swiftly to changing scenarios, such as the enhanced 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, a demand which the ECCF can fulfil. Furthermore, the ECCF's linkage with emerging legislative acts, notably the CRA (Cyber Resilience Act) and NIS2 (Network and Information Security) Directive, highlights its anticipated value in addressing critical infrastructure needs and legal conformity across the EU. ENISA's proactive role and the establishment of National Cybersecurity Certification Authorities mark crucial milestones toward strengthening collaborative interactions and promoting certification adoption. However, the gaps in resource allocation and expertise between larger and smaller Member States continue to perpetuate imbalances in participation and effectiveness, impacting collective scheme development.

Coherence

The ECCF's coherence is also 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. The complete coherence of the ECCF with other EU legislative instruments, including the NIS2 Directive and the CRA, is crucial to ensuring a unified cybersecurity approach. The ECCF exhibits a theoretical alignment 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 EU common criteria (EUCC) scheme poses a significant test for this coherence, as its successful deployment will demonstrate the ECCF's ability to harmonise and effectively leverage additional legislative efforts. Stakeholders have underscored the need for careful coordination between the ECCF and emerging regulatory acts to prevent overlaps, which could undermine efficiency and dilute intended impacts across sectors. Specifically, concerns arise regarding the interface between the ECCF and the CRA, as both initiatives aim to enhance cybersecurity standards but risk redundancy if not applied in a complete synergy where one legislation supports and complements the other. On the sectoral side, coherence must extend to accommodate continuing advancements in technology, ensuring that cybersecurity initiatives are appropriately nuanced to address critical infrastructure needs.

EU Added Value

Despite its potential, the ECCF has struggled to deliver its 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 advance in the EU's ability to create a harmonised approach to the certification of ICT products, services and processes. This framework's inherent EU added value 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 scheme implementations 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 EU common criteria (EUCC), curtailed immediate impacts, leaving its theoretical potential largely unfulfilled. 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. 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 among ENISA, Member States and industries, strengthening its 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 Member State cooperation 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 complexity and political pressures from industry lobbying. These delays undermine trust and prevent swift adoption of European cybersecurity certification schemes. 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 affect the framework's efficacy, 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.

3. CONCLUSIONS AND RECOMMENDATIONS

3.1 ENISA

The evaluation of ENISA highlights its crucial role in working towards a cohesive cybersecurity landscape across the EU. ENISA has shown effectiveness and generated valuable outputs. As demands on ENISA continue to grow, it is important to reassess and streamline its operations to better align resources and priorities, with continued emphasis on supporting Member States as they address cybersecurity threats and enhance national cybersecurity infrastructures. Refining its report production process, making them more user-friendly and accessible through visual aids and concise summaries could enhance ENISA's effectiveness and relevance in the current threat landscape. 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 could aid in fostering stronger connections and cooperation within existing cybersecurity networks such as ISACs.

ENISA can improve efficiency through a more strategic focus on task prioritisation, enabling a more streamlined approach to managing workload pressures. To improve relevance amongst stakeholders, ENISA's central role in supporting Member States should continue to be elevated by strengthening its capacity of providing timely insights into emerging threats and strategic tools for addressing them. Moreover, as indicated by a number of stakeholders, ENISA could establish more structured and transparent methods of engaging with private entities, including supporting SMEs. Clarity regarding ENISA's role in policy implementation with other EU institutions should be sought, 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 enhance 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. These recommendations aim to enhance ENISA's capacity to effectively manage its responsibilities and reaffirm its role as a leading entity in cybersecurity.

3.2 ECCF

The evaluation of the ECCF reveals several strategic recommendations. Firstly, 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 for a substantial revision in governance structures to enhance operational clarity and accountability at all levels.

To address these findings, several actions are recommended to optimise ENISA's contribution to the ECCF. There should be a concerted effort to ensure a consistent and adequate distribution of financial and human resources across ENISA and other stakeholders within the ECCF. Stabilising employment arrangements is essential to reduce turnover and enhance institutional memory, thereby facilitating efficient scheme implementation and ongoing maintenance. Developing streamlined decision-making processes within the ECCF, which clarify roles and responsibilities, will promote transparency and efficiency, particularly in enhancing collaborative efforts among Member States, the Commission, and ENISA. This will foster accountability and reduce inefficiencies. 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.

Furthermore, actively investing in 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. Additionally, industry and consumer awareness should be increased through targeted campaigns and strategic involvement, emphasising the value of certified products and services. A proactive approach in garnering stakeholder support is critical to boosting demand and trust in ECCF initiatives.