SPECIAL REPORT 19/2026 **EN**

Detecting and responding to cybersecurity incidents

EU cooperation framework progressing, but only partially effective due to implementation delays and limited information sharing

CURIA RATIONUM
EUROPEAN COURT OF AUDITORS

Contents

Paragraph

Annexes

Abbreviations

Glossary

Replies of the Commission

Replies of the European Cybersecurity Competence Centre (ECCC)

Replies of the European Union Agency for Cybersecurity (ENISA)

Timeline

Audit team

01

Main messages

Why this area is important

01 The risks for cyberattacks increase as our economy and our day-to-day lives become more digitalised. Cybersecurity is defined as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"[1]. Cybersecurity requires a holistic approach to prevent, detect, respond to, and recover from cyber threats.

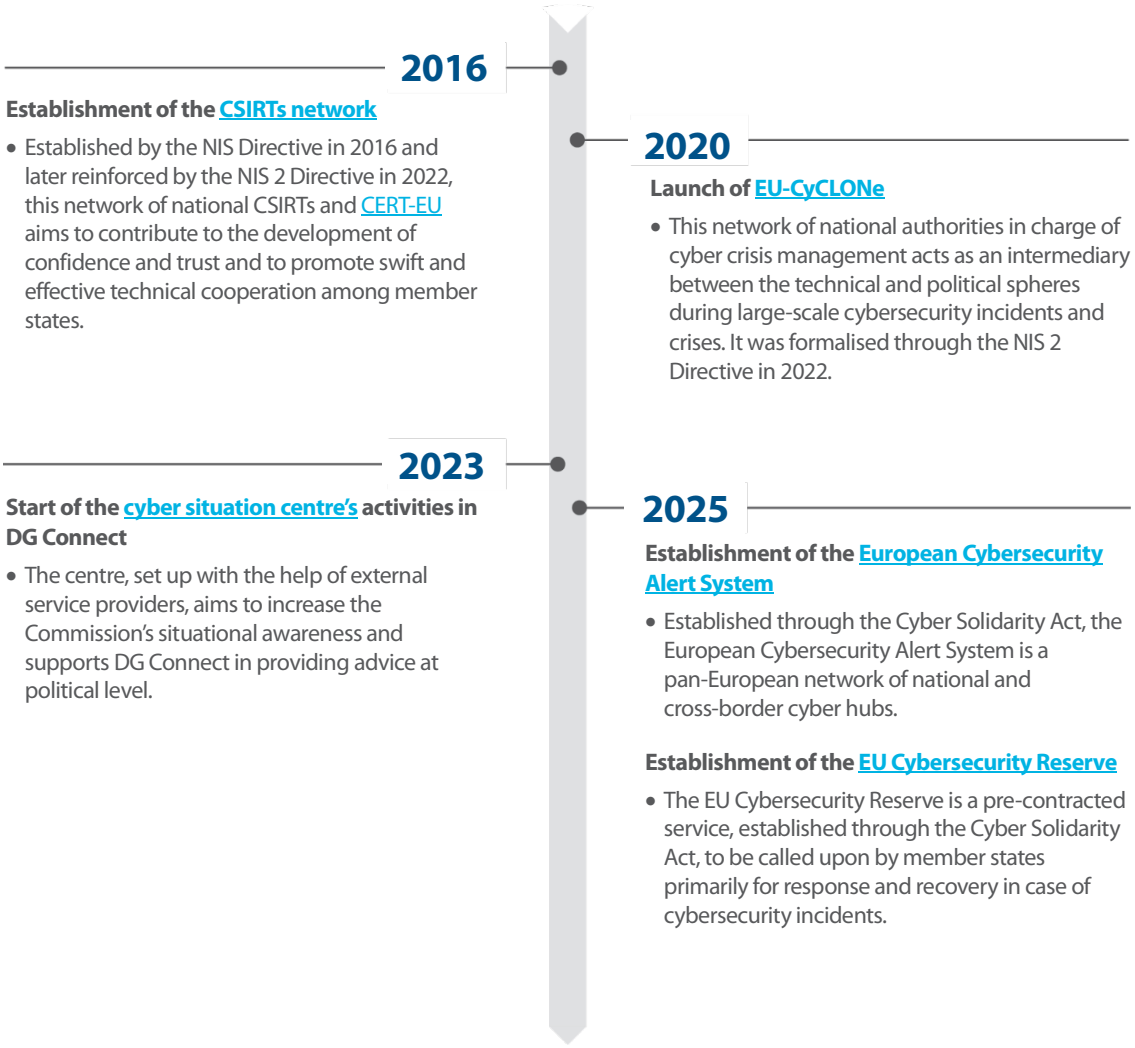
02 The EU cybersecurity landscape involves numerous public and private entities at regional, national and EU level in the civilian sphere. Cybersecurity is also a key element of national security and defence.

03 Member states bear primary responsibility for preventing, preparing for, and responding to cybersecurity incidents and crises affecting them. As these incidents can affect the smooth functioning of the internal market, the EU also plays an important role in the event of a significant incident or crisis. In recent years, the EU has reinforced its evolving cybersecurity regulatory framework[2] and established networks and mechanisms, as illustrated in ***Figure 1*** below and ***Annex II***.

[1] Regulation (EU) 2019/881 (Cybersecurity Act).

[2] For example, the Commission proposed the Digital Omnibus in November 2025 and a revised EU Cybersecurity Act in January 2026.

Figure 1 | EU cybersecurity networks and mechanisms 2016-2025



CSIRTs: computer security incident response teams
DG Connect: Directorate-General for Communications Networks, Content and Technology
EU-CyCLONe: European Cyber Crisis Liaison Organisation Network
NIS Directive: Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
NIS 2 Directive: Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union

Source: ECA.

04 Under the current 2021-2027 multiannual financial framework, the main source of funding for cybersecurity is the Digital Europe Programme (DIGITAL). It has a total budget of €8.1 billion, out of which €1.4 billion is allocated to strengthening cybersecurity.

05 The objective of our audit was to assess whether EU actions facilitate the detection of and response to significant and large-scale cybersecurity incidents effectively. We assessed whether this was the case for:

- EU-level networks and mechanisms (i.e. the network of computer security incident response teams (CSIRTs network), the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe), the European Cybersecurity Alert System, the cyber situation centre, and the EU Cybersecurity Reserve);
- actions funded under DIGITAL.

06 We expect our findings to contribute to strengthening the EU's cyber resilience by improving the effectiveness and efficiency of the EU networks and mechanisms, as well as improving the way EU-funded actions are selected and monitored.

07 The audit covers the period from 2022 to 2025. It is based on a desk review and analysis of relevant documents, audit visits to three member states (Ireland, Greece and Italy), and written questionnaires and interviews with relevant stakeholders. More background information and details on the audit scope and approach can be found in ***Annex I***.

What we found and recommend

08 Overall, we conclude that EU actions only partially facilitate the detection of and response to significant and large-scale cybersecurity incidents. While a cooperation framework has gradually been put in place, work is still ongoing towards achieving full set-up. Limited information sharing, reporting weaknesses and considerable implementation delays prevent EU networks and mechanisms from reaching their full potential. Projects funded by DIGITAL pursue relevant objectives, but several face operational challenges and delays, and there are weaknesses in the overall performance monitoring framework.

09 The current framework of EU networks and mechanisms to facilitate the detection of and response to significant cybersecurity incidents was built up gradually. In 2025, the Council adopted the Cyber Blueprint, setting out the EU framework for cyber crisis management. We found that the Cyber Blueprint largely clarifies roles and responsibilities as regards EU cyber crisis management. This notwithstanding, the procedural arrangements as to how the CSIRTs network (established in 2016) and EU-CyCLOne (formalised in 2023) should work together, are yet to be formalised (paragraphs ***24***-***30***).

10 We found that information sharing through these networks is limited. This is mainly due to delays in the transposition of the Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive), difficulties in determining whether an incident has a cross-border impact, and national security legislation preventing information sharing. The added value of the networks is significantly reduced if member states are not willing to share timely and actionable information (paragraphs ***31***-***44***).

Recommendation 1

Strengthen information sharing between member states

To improve the detection of and response to cybersecurity incidents, the Commission, with the support of the European Union Agency for Cybersecurity (ENISA), should:

(a) propose, to the Network and Information Security Cooperation Group, that it carry out a detailed analysis of national security restrictions that limit information sharing and affect the EU's cyber resilience, and that it identify legal and technical solutions to increase information sharing while respecting the boundaries of national security;

(b) without prejudice to the decisions of the co-legislators, ensure, in collaboration with member states, that the single-entry point for incident reporting proposed by the Digital Omnibus can detect potential cross-border incidents;

(c) work on solutions to enable real-time incident reporting to ENISA.

Target implementation date: (a) and (b) 2027, (c) 2028

11 In 2022, the Commission established its "cyber situation centre" sector to increase its situational awareness, with the aim of supporting its institutional responsibilities for crisis management. The functioning of the centre is largely supported through a contract with external service providers. We found that the work performed by the external service providers partly duplicates the existing capacity of the European Union Agency for Cybersecurity (ENISA) regarding situational awareness and threat monitoring. We consider that the way the cyber situation centre was set up did not sufficiently exploit the potential for rationalisation by making use of information already available from the Commission and ENISA. Furthermore, the absence of a comprehensive, detailed plan for the future after the contract expires poses a risk to the cyber situation centre's operation after 2026 (paragraphs ***45***-***51***).

Recommendation 2

Rationalise EU cybersecurity situational awareness capabilities and optimise the dissemination of information

To increase efficiency, the Commission should, in collaboration with ENISA, assess the feasibility of joint acquisition and analysis of information for situational awareness. It should also make this information and the related cyber threat reports available across relevant departments and agencies of the EU.

Target implementation date: 2027

12 The 2024 Cyber Solidarity Act establishes the EU Cybersecurity Reserve, which aims to support member states in responding to and recovering from major cybersecurity incidents. It consists of selected service providers for each member state, able to respond to incidents around the clock. While this approach helps to address member states' specific requirements and to build trust, the available budget is divided equally between them and does not take account of the specific needs of each member state (paragraphs ***52***-***57***).

13 We consider that the use of pre-contracted providers enables a quick deployment of incident response services. Although the EU Cybersecurity Reserve primarily aims to support response and recovery, when not used for incident response, it can be used for preparedness. This flexible approach can prevent pre-paid services from being unused. However, the Reserve risks being predominantly used for preparedness rather than response, contrary to its intended purpose (paragraphs ***58***-***61***).

14 The European Cybersecurity Alert System is a network of national and cross-border cyber hubs that aim to improve the detection, analysis and response to cyber threats. We found that, at the time of the audit, due to considerable delays in the procurement of tools and services, the two hubs (ATHENA and ENSOC) were not yet operational and that the European Cybersecurity Alert System was not yet functioning (paragraphs ***62***-***70***).

15 One of the key objectives of the European Cybersecurity Alert System is to encourage meaningful information sharing among clusters of member states. While this has the potential to resolve some of the issues related to information sharing, it is also very challenging to integrate cyber hubs into the already complex cybersecurity landscape. We found that the required cooperation agreements, common taxonomy, and interoperability standards needed for the full functioning of the European Cybersecurity Alert System were not yet in place (paragraphs ***71***-***74***).

Recommendation 3

Integrate the European Cybersecurity Alert System into the EU cybersecurity landscape

The Commission should, together with ENISA and member states, ensure that cooperation arrangements and interoperability standards are in place to facilitate information sharing among cross-border hubs that are part of the European Cybersecurity Alert System, the CSIRTs network, and EU-CyCLONe.

Target implementation date: 2028

16 In 2018, the Commission proposed the creation of the European Cybersecurity Competence Centre (ECCC) to manage the cybersecurity component of DIGITAL starting from 2021. The ECCC Regulation called for the creation of a Cybersecurity Competence Community comprising representatives from industry, academic and research organisations. Selected members from the Cybersecurity Competence Community would then form a Strategic Advisory Group (SAG) (paragraphs ***75***-***76***).

17 We found that there were delays in the ECCC reaching financial autonomy, and in the establishment of the Cybersecurity Competence Community and the SAG. This meant that the Cybersecurity Competence Community and the SAG could not provide their input to shape the DIGITAL work programmes. We consider that this was a missed opportunity (paragraphs ***77***-***81***).

18 We found that all the projects we examined pursued relevant objectives that contribute to achieving the DIGITAL cybersecurity objectives. However, we found cases where the quality or the results achieved were not satisfactory, mainly due to implementation delays (paragraphs ***82***-***87***).

19 The DIGITAL Regulation provides that, for security reasons, funding for cybersecurity may be restricted to entities that are established in the member states and controlled by member states or by nationals of member states. The Central Validation Service at the European Research Executive Agency performs this ownership and control assessment on the ECCC's behalf (paragraphs ***88***-***91***).

20 In the case of financial support to third parties, the ownership and control assessment is the project beneficiaries' responsibility, based on their own approach and methodology. We found that the ECCC does not validate their methodology, nor perform checks to ensure that selected third parties are EU-owned and controlled. We consider that there is a significant risk that beneficiaries do not have the capacity to perform these checks properly. This risk has not been adequately mitigated and could lead to the exposure of sensitive infrastructure, operational data, and security-critical technologies (paragraphs ***92***-***96***).

Recommendation 4

Ensure a robust ownership and control assessment of entities receiving EU funding under the Digital Europe Programme

The European Cybersecurity Competence Centre should:

(a) obtain reasonable assurance that beneficiaries responsible for providing financial support to third parties have the administrative and technical capacity necessary to perform adequate ownership and control assessments, based on the existing methodology available to beneficiaries implementing financial support to third parties; and

(b) check, on a sample basis, whether only eligible entities have received EU funding.

Target implementation date: (a) 2026, (b) 2027

21 Beneficiaries managing EU-funded projects must report on their progress and results to the ECCC, using milestones and deliverables. These are key to project monitoring and should be defined properly. We found that almost none of the projects in our sample followed the instructions on how to draw up milestones and deliverables, and that many of them were not useful for tracking progress (paragraphs ***97***-***99***).

22 We found that many of the performance indicators used by beneficiaries are not relevant or measurable and lack a target or a baseline. Furthermore, the reporting on these indicators was inadequate and therefore cannot serve as a basis for assessing project performance (paragraphs ***100***-***102***).

23 To monitor the achievements of DIGITAL as a whole, all projects must report on specific programme indicators that feed into the Commission's annual programme performance statements. The ECCC is responsible for collecting and verifying the data provided on these indicators. We found several problems in the way data was collected and its overall quality.

We found no evidence that the accuracy of the reported data was verified by the ECCC. Based on our sample checks, we consider that the reported data does not accurately reflect the achieved results (paragraphs ***103***-***106***).

Recommendation 5

Strengthen the performance monitoring framework of the cybersecurity component of the Digital Europe Programme

To enable adequate progress and performance monitoring, the European Cybersecurity Competence Centre should:

(a) ensure, prior to grant signature, that all projects have defined milestones, deliverables, and performance indicators that comply with the instructions provided in the application form;

(b) design and implement a robust system for the collection, traceability, verification, and aggregation of the data for the performance indicators of the cybersecurity component of the Digital Europe Programme, to ensure the indicators accurately reflect the results achieved.

Target implementation date: 2027

02

A closer look at our observations

While EU cybersecurity networks and mechanisms support cooperation and response, limited information sharing and incomplete implementation reduce their effectiveness

EU networks enable member state cooperation, but limited information sharing reduces their added value

24 The current EU framework of networks and mechanisms to facilitate the detection of and response to significant cybersecurity incidents was built up gradually, starting with the Directive concerning measures for a high common level of security of network and information systems across the Union[3] (NIS Directive), which came into force in August 2016. We illustrate the current EU landscape in ***Annex II***.

EU networks enable member state cooperation at the technical and operational levels

25 The NIS Directive established the CSIRTs network, which brings together CERT-EU (the Cybersecurity Service for the Union institutions, bodies, offices and agencies) and the CSIRTs appointed by member states. This network aims to build confidence and trust between national CSIRTs and promote swift and effective operational cooperation between member states.

---

[3] Directive (EU) 2016/1148.

26 EU-CyCLONe was established in 2020 as an informal cooperation network for national authorities in charge of cyber crisis management. It serves as a bridge between the technical layer at which the CSIRTs network operates and the political layer of the Council of the European Union and its integrated political crisis response arrangements. The entry into force of the NIS 2 Directive in 2023 formalised the role of EU-CyCLONe and gave it a clear mandate.

27 We assessed whether the roles and responsibilities of these EU-level networks are well defined, and whether they enable member states' cooperation.

28 ENISA acts as the secretariat of the CSIRTs network and EU-CyCLONe and provides them with resources, expertise, infrastructure and the IT tools necessary for cooperation and secure communication for information sharing. In its stakeholder satisfaction survey[4] from early 2025, ENISA received good scores for its performance as the secretariat for these networks. This positive feedback was also confirmed during our audit visits, where national cybersecurity authorities expressed their appreciation.

29 In 2025, the Council adopted the Cyber Blueprint, which defines the roles and responsibilities of the key actors (including the CSIRTs network and EU-CyCLONe) and mechanisms involved throughout large-scale cybersecurity incidents or cyber crises. We found that the Cyber Blueprint largely clarifies roles and responsibilities as regards EU cyber crisis management and takes into account the changes in the landscape since the first blueprint in 2017. It defines three levels of cooperation: technical, operational, and political. It details the new networks and structures established since 2017 – such as EU-CyCLONe, the EU Hybrid Rapid Response Teams, and the European Cybersecurity Alert System – and it addresses how cyber crisis management should be integrated into the EU's broader crisis response framework.

30 However, despite the official establishment of the CSIRTs network in 2016 and EU-CyCLONe in 2023, the two networks have yet to formalise the procedural arrangements on how they should work together. They have also not agreed on the criteria for the CSIRTs network to advise EU-CyCLONe that an observed cybersecurity incident constitutes a potential or ongoing large-scale cybersecurity incident. The two networks also have to agree on a common taxonomy of incident severity levels and key concepts – such as "threat", "threat actor", "incident", or "impact" – which is necessary to enable automated information exchange. Currently, there is room for interpretation as to when an incident qualifies as significant or large-scale. The lack of a common taxonomy was mentioned by the cybersecurity authorities of all three member states we visited.

---

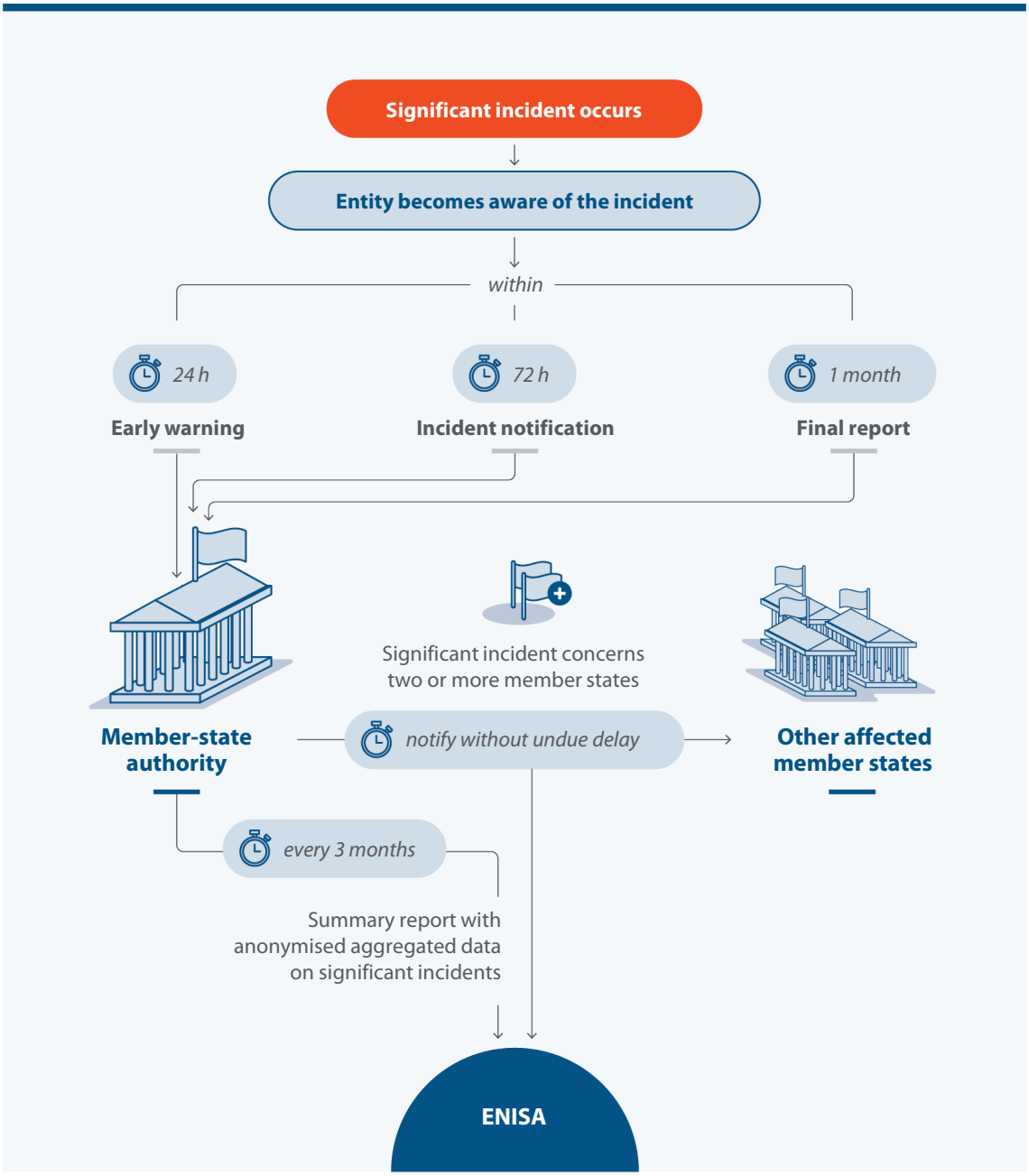
[4] ENISA 2024 consolidated annual activity report, pp. 33 and 36.

Limited information sharing and reporting significantly reduce the added value of these networks

31 Geographical borders do not prevent cybersecurity incidents and cyberattacks from occurring and spreading. Information sharing between member states on, for example, the tactics and techniques used by threat actors, and on digital signs that a network or information system has been breached ("indicators of compromise"), can contribute significantly to increased cybersecurity.

32 We found that information sharing was limited, significantly reducing the added value of these networks. The limitations we observed mainly concern delays in the transposition of the NIS 2 Directive, issues with determining whether an incident has a cross-border impact, national security legislation curtailing information sharing, and a lack of trust. The NIS 2 Directive introduces several reporting requirements for entities under its scope and for member-state authorities, as illustrated in ***Figure 2***.

Figure 2 | Incident reporting time frame under the Directive on measures for a high common level of cybersecurity across the EU (NIS 2)



Source: ECA, based on ENISA.

33 Member states had until October 2024 to transpose the NIS 2 Directive into national law, but only two met the deadline. Delays in transposition have a significant impact on information sharing because, in the meantime, the entities covered by the NIS 2 Directive are not legally required to report incidents. The Commission estimated[5] that 15 500 entities were covered by the NIS Directive, whereas over 110 000 fall under the scope of the NIS 2 Directive. For example, public administration – the most targeted sector in the EU, according to ENISA's 2025 threat landscape report – had no obligation to report incidents under the NIS Directive.

34 The reporting of incident data to ENISA every three months (i.e. long after an incident may have taken place) limits its added value. This data mostly serves for statistical purposes and historical trend reporting, not to improve detection and response. ENISA provides member states with an online tool to submit their reports. The reporting template contains a minimum set of data that must be provided, such as the type of incident and the sector involved. In addition, ENISA suggests that member states provide additional information to allow for a more in-depth analysis of the data, for example by linking incidents to specific vulnerabilities. However, not all member states choose to provide this information, significantly reducing the quality and added value of the data collected.

35 ENISA, in its 2024 report on the state of cybersecurity in the EU, stated that incidents are probably underreported, as the number of reported incidents seemed to be low. In the years 2018 to 2021 member states reported between 100 and 500 incidents annually to ENISA. The number has been increasing gradually and, in 2024, it rose to 1 276[6].

36 In its 2025 threat landscape report, which covers the period from June 2024 to June 2025, ENISA identified approximately 4 800 cybersecurity incidents[7] through open-source intelligence such as news articles. These incidents would not have all been reportable under the NIS 2 Directive as, when collecting the data, ENISA covers a broader spectrum of incidents. Conversely, many significant incidents are not reported in open-source intelligence. As the data reported by member states is anonymised, ENISA cannot correlate the incidents it identifies to those reported by member states. It is therefore not possible to determine the extent of underreporting accurately, but we consider that the difference between the number of incidents reported by member states and those in the threat landscape report shows that not all significant incidents are reported.

---

5 European Commission, 2020 impact assessment report.

6 CIRAS data for 2024.

7 ENISA's 2025 threat landscape report.

37 Another indication of underreporting is the number of notifications to other affected member states and ENISA concerning significant cross-border incidents. A similar requirement existed under the NIS Directive but was deemed ineffective, as the Commission concluded[8] in 2020 that notifications were rarely sent despite the obligation. It attributed the failure to notify to the lack of clear modalities for information sharing and the absence of common objectives incentivising sharing.

38 The obligation to inform other member states is crucial to prevent the spillover of incidents – not doing so negatively affects the EU's cybersecurity. In 2025, only 14 significant cross-border incidents were reported, by seven member states. Member states submitted two incident reports in 2024, none in 2023, and three in 2022 with possible cross-border impact. This shows that the reporting of significant cross-border incidents is very low and does not reflect the true extent of such attacks. To put this into perspective, in its 2024 threat landscape report, ENISA identified 322 incidents specifically targeting two or more member states. The Collins Aerospace incident (see ***Box 1***) is an example of member states not reporting an incident despite it having a significant cross-border impact.

Box 1

Cybersecurity incident disrupting airport operations

In September 2025, Collins Aerospace, a major technology provider for the aviation industry, suffered a significant ransomware attack that targeted its passenger processing software. The attack forced major European airports to revert to manual operations, causing widespread flight delays and cancellations. The disruption was most severe at London Heathrow Airport, Brussels Airport, Berlin Brandenburg Airport, and Dublin Airport.

According to the NIS 2 Directive, an incident is considered "significant" if, among other things, it causes severe operational disruption to the services or financial loss to the entity concerned. Yet, no member state treated this incident as being either significant or large-scale cross-border. Therefore, none of the affected member states formally notified ENISA or other member states of the incident. The CSIRTs network did not advise EU-CyCLONe, which therefore did not support the coordinated management of the incident.

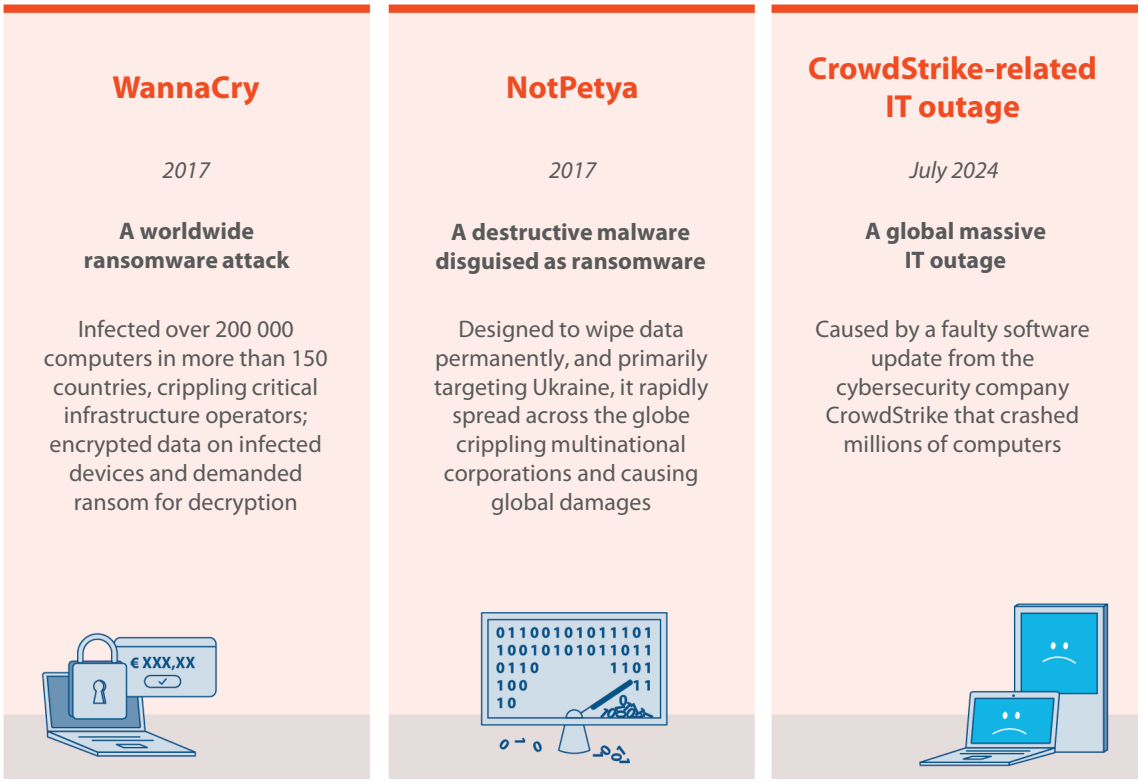
Source: ECA analysis based on interviews with ENISA.

[8] European Commission, 2020 impact assessment report.

39 Another reason for the limited reporting of cross-border incidents is that it is up to each member-state authority to determine whether a reported incident has a cross-border impact, and to identify the other affected member states. Based on the information available to them, the reporting entity or the member-state authority might not be aware of the cross-border nature of some attacks. Currently, there is no EU-wide platform that receives real-time incident reports from all member states and that could correlate information on sectors or indicators of compromise to detect cross-border incidents. There is therefore a significant risk that some cross-border incidents might not be identified and reported.

40 No cybersecurity incident has been considered "large-scale" by any member state since 2016. In principle, any incident that significantly affects at least two member states falls under that definition. However, even cybersecurity incidents that have caused global outages and significant damage, such as those shown in ***Figure 3***, have not been considered large-scale. As a result, the EU-CyCLONe escalation procedure has never been fully activated due to a large-scale cybersecurity incident.

Figure 3 | Examples of major cybersecurity incidents



Source: ECA, adapted from Cloudflare, ENISA, Europol, Wired, IBM, CrowdStrike.

41 In addition to the reporting obligation imposed on entities and member states, the CSIRTs network was created to facilitate information sharing. Trust between member states is at the core of the CSIRTs network, where information is shared on a voluntary basis. The

added value of the network is significantly reduced if member states are not willing to share timely, actionable information.

42 Information sharing at EU level is restricted by the national security legislation of each member state. If a member state considers that cyberattack-related information on a critical entity is classified, or that reporting on a specific incident would be detrimental to its national security, it is under no obligation to share the information. During our visits to member states, representatives of the CSIRTs network and EU-CyCLONe stated that sharing can only be done within the boundaries of national security legislation. An analysis of member states' national legal frameworks and their impact on information sharing has not been performed at EU level.

43 In 2016, the CSIRTs network comprised 28 national CSIRTs, with two representatives per member state. The lack of information sharing has been a persistent issue, and the Commission's evaluation of the NIS Directive recognised that "member states do not share information systematically with one another", which particularly affects the effectiveness of the cybersecurity measures and the level of joint situational awareness at EU level. Under the NIS 2 Directive, many member states have appointed sectoral CSIRTs in addition to their national CSIRT, so the network has expanded significantly. At the time of the audit, it comprised 42 CSIRTs and over 700 individual participants. This makes building trust even more challenging, as maintaining close links among all members is difficult.

44 The CSIRTs network is aware of the information-sharing issue and is considering various actions to increase trust in a growing network. The creation of smaller clusters of member states forming cross-border hubs, as detailed in paragraphs ***62***-***74***, is an alternative approach to an EU-wide network that may help address this challenge.

The cyber situation centre's contracted services partly duplicate existing capacities and its future functioning is not clear

45 Under the NIS 2 Directive, in cases where a potential or ongoing large-scale cybersecurity incident has or is likely to have a significant impact, the Commission becomes a member of EU-CyCLONe[9]. This new role, and the evolution of the threat landscape, led the Commission to establish a Cyber Coordination Task Force within DG Connect in 2022. This task force includes a cyber situation centre, which should help the Commission to increase its situational awareness, with the aim of supporting its institutional responsibilities for crisis management. It should also help DG Connect to provide advice at a political level.

[9] Article 16(2) of NIS 2 Directive.

46 To set up the cyber situation centre, the Commission is largely supported by external service providers contracted in December 2022 for nearly €18 million over four years. We assessed the centre's establishment, its outputs, and the Commission's plans for its future functioning.

47 As part of the services provided, the contractors have set up a dashboard based on commercial cyber threat intelligence feeds in order to present and share threat information. They also produce various cyber threat intelligence reports, including daily and weekly reports, and thematic reports on countries or on sectors of the economy. The physical cyber situation centre, which consists of a room equipped with workstations remotely connected to the dashboard hosted by the contractors, has been set up in one of the Commission's buildings. At the time of the audit, the cyber situation centre comprised a small number of Commission staff, supported by many analysts from the contractors as well as experts from ENISA.

48 We found that the work performed by the external service providers for the cyber situation centre partly duplicates ENISA's existing capacity. ENISA has permanent capacity for situational awareness and threat monitoring. It regularly publishes cyber threat reports, including flash reports on specific incidents, and weekly reports that provide an overview of threats. The reports are based on open-source intelligence and are similar to those produced by the contractors. Additionally, ENISA produces or contributes to high-level briefs for policymakers during times of crisis, which are also comparable to what the cyber situation centre produces.

49 Furthermore, the data used by the cyber situation centre to produce these reports is based on commercial cyber threat intelligence feeds and is similar to the data used by other Commission departments, such as the Directorate-General for Digital Services, and CERT-EU. We consider that the way the cyber situation centre was set up did not sufficiently exploit the potential for rationalisation by making use of already available information from the Commission and ENISA.

50 The contract expires in December 2026, after which the contractors will no longer provide the services for the cyber situation centre. These services include providing the data available in the dashboard, producing the threat reports, and making up the majority of the centre. The dashboard will be handed over to the Commission but will lose its added value if not continuously updated with cyber threat intelligence.

51 At the time of the audit, the Commission had no plans concerning the support by the external service providers for the operation of the cyber situation centre once the contract expires. We consider that the absence of a comprehensive, detailed plan for the future after the contract expires poses a risk to the cyber situation centre's operation after 2026.

The EU Cybersecurity Reserve enables the quick deployment of incident response services

52 In 2022, in the immediate wake of Russia's military aggression against Ukraine and acknowledging that large-scale cyberattacks have become more prevalent, the Commission provided ENISA with €15 million in exceptional funding to pilot the Cybersecurity Support Action, which was launched in 2023. In 2023, the Commission provided additional funding (approximately €20 million) to extend the programme until the end of 2026.

53 The Commission also proposed the Cyber Solidarity Act – adopted in December 2024 – to prepare for facing large-scale cybersecurity incidents. The Act establishes an EU Cybersecurity Reserve that comprises incident response services from trusted providers. It began operating gradually in 2025, with a budget of €36 million for the 2025-2027 period.

54 We assessed how the Cybersecurity Support Action programme was organised, as it forms the basis for the EU Cybersecurity Reserve. We also checked whether the lessons learned since 2022 have fed into the design of the EU Cybersecurity Reserve.

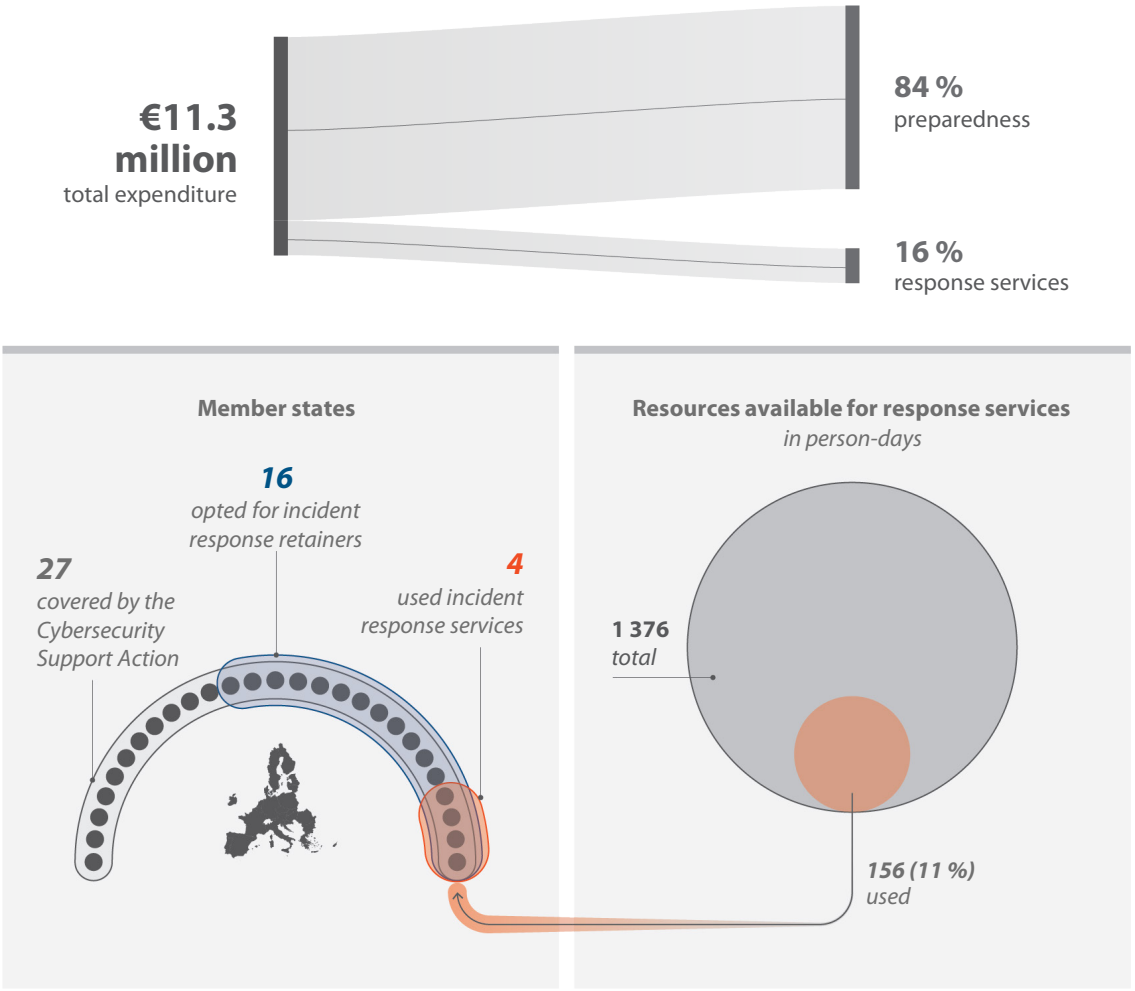
55 ENISA designed the Cybersecurity Support Action as a mechanism to provide services to support member states' preparedness and response to large-scale cybersecurity incidents or crises. All services are pre-contracted by ENISA, which means that service providers can start working as soon as member states require them. This is also due to ENISA's set-up, which ensures that there is an officer on call around the clock to deal with member states' requests.

56 ENISA chose to allocate the available budget equally among member states. In practice, the agency launched an open tendering procedure divided into 27 lots, one per member state, to select up to three private security providers to deliver services until the end of 2026. In addition, ENISA selected some providers under a pan-European lot to provide services to eligible non-EU countries, as well as EU institutions, bodies and agencies, or to support the response to cross-border incidents.

57 This approach enabled ENISA to take into account specific national requirements, including language, national security clearances, or established presence in the member states. On the other hand, as providers were not selected to be able to deliver services across the EU, a major drawback of this approach is that if a member state does not use the pre-contracted services, the budget committed for such services for a specific member state cannot be used to assist another member state.

58 For the Cybersecurity Support Action, member states could choose between preparedness or response services, or a combination of both. Member states primarily opted to use the available funding to improve their preparedness (84 % of the expenditure in 2023). Member states who opted to have an incident response retainer (i.e. a predefined agreement with a provider that ensures the member state can access the provider's services on demand for swift cybersecurity incident response) used it sparingly, as shown in ***Figure 4***. In the three visited member states, authorities expressed appreciation for ENISA's management of the Cybersecurity Support Action.

Figure 4 | ENISA Cybersecurity Support Action until 2023



Source: ECA, based on ENISA data.

59 For the 2024-2026 period, only nine member states have requested an incident response retainer. Our interviews with ENISA and authorities in three member states have confirmed a strong preference for preparedness activities.

60 Although the EU Cybersecurity Reserve primarily aims to support response and recovery as regards major cybersecurity incidents, pre-committed services from the EU Cybersecurity Reserve not used for incident response can be converted into preparedness services. This flexible approach can prevent pre-paid services from being unused.

61 We consider that the model chosen for the EU Cybersecurity Reserve draws from the lessons learned from the Cybersecurity Support Action programme. However, the data on the use of the Cybersecurity Support Action programme points to a risk that the EU Cybersecurity Reserve might be primarily used for preparedness and not response, contrary to the purpose laid out in the Cyber Solidarity Act.

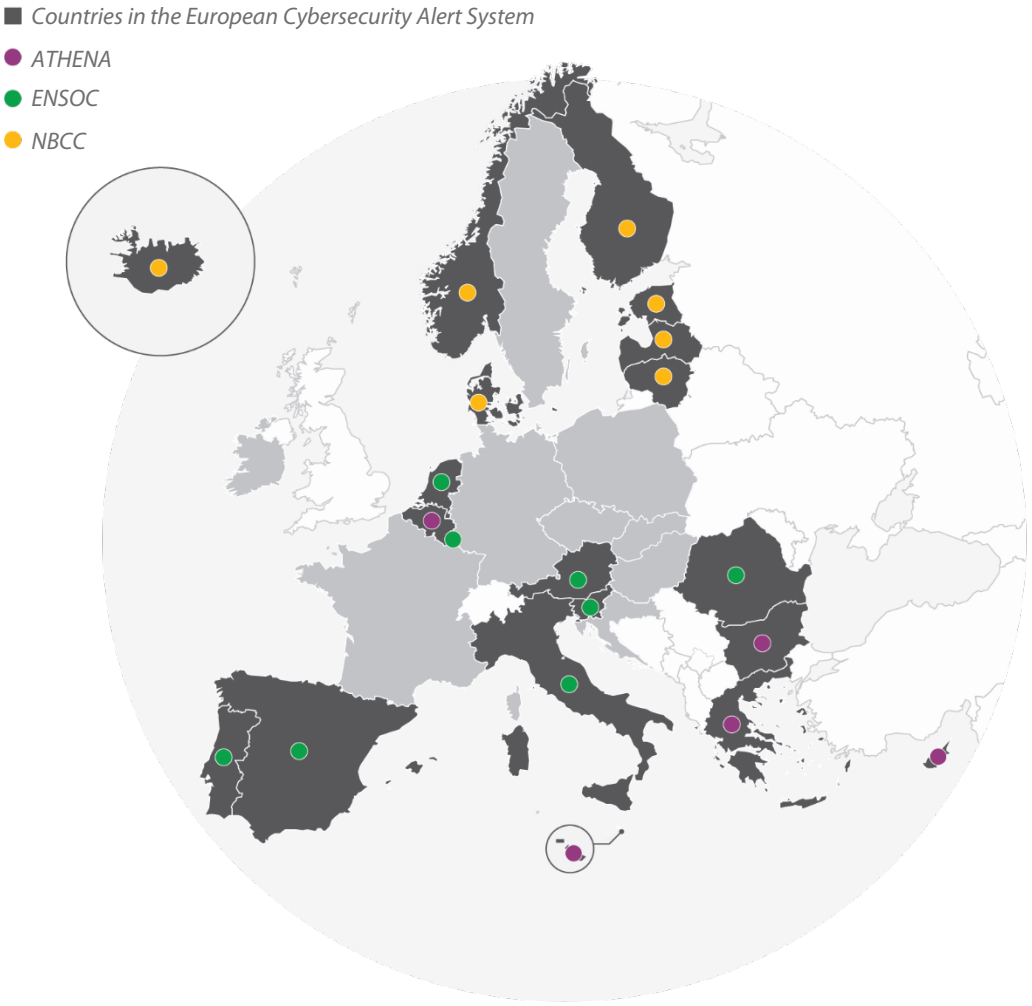
The European Cybersecurity Alert System aims to improve threat detection capacities but is not operational

62 One of the key objectives of the European Cybersecurity Alert System is to encourage meaningful information sharing to improve the detection, analysis, and response to cyber threats. Participation in the alert system is voluntary, but member states that choose to join a cross-border cyber hub must commit to sharing relevant information with the other members. By working together in clusters in a trusted and secure environment, member states might avoid some of the issues related to information sharing identified in paragraphs ***31-44***.

63 At the time of the audit, 13 member states had opted to be part of the European Cybersecurity Alert System, establishing two cross-border hubs: ATHENA and ENSOC. A third cross-border cyber hub, NBCC, had been allocated funding for its establishment in 2026, bringing the network's membership to a total of 20 countries (18 member states, as well as Iceland and Norway[10]), as shown in ***Figure 5***.

[10] Associated non-EU countries in accordance with Article 10(1)(a) of Regulation (EU) 2021/694.

Figure 5 | Countries in the European Cybersecurity Alert System



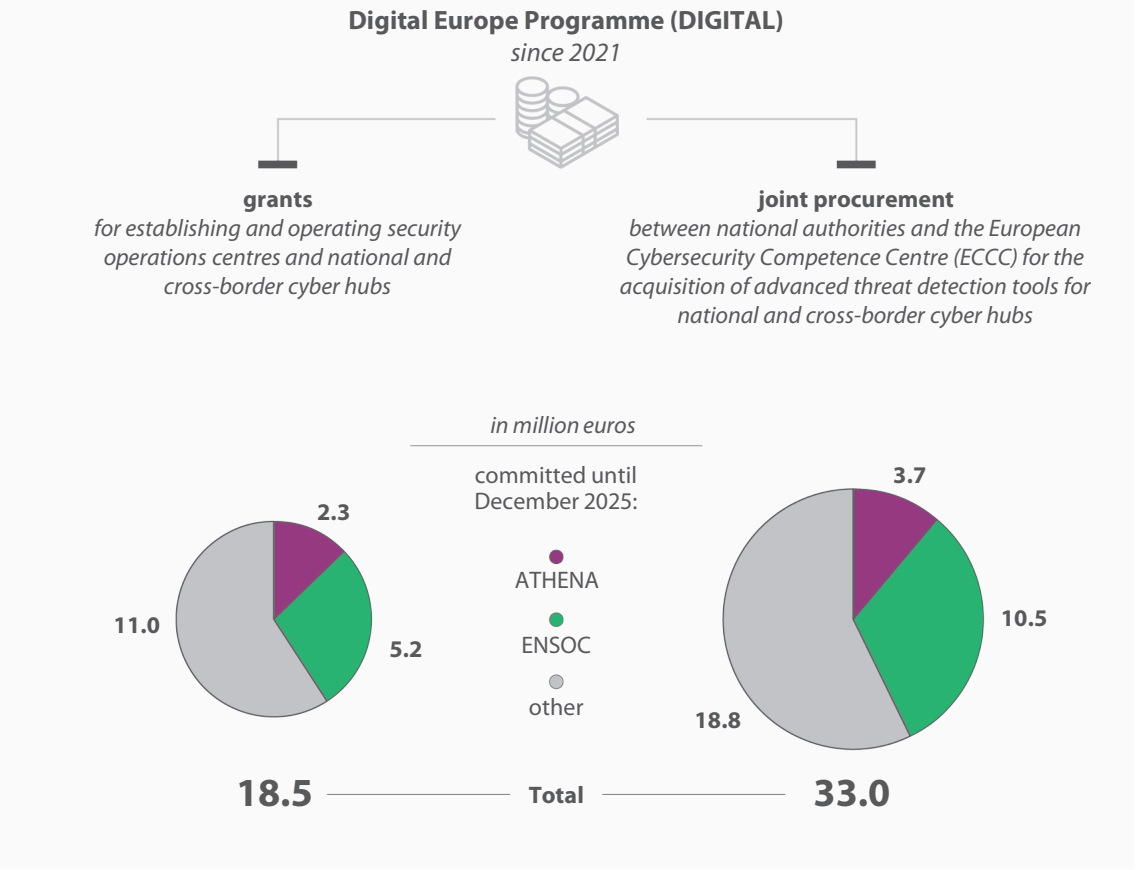
Source: ECA.

64 We assessed how the first two cross-border cyber hubs have been set up, as well as their progress towards the objectives of the European Cybersecurity Alert System. We also examined how the establishment of the cross-border cyber hubs fits into the broader cybersecurity landscape and interacts with existing networks and structures.

No concrete results achieved so far, due to considerable delays in procurement

65 Funding to support the establishment of national and cross-border cyber hubs has been available through DIGITAL since 2021. This funding is provided through a complex procedure with two parallel streams: traditional grants to support the hubs' establishment and operation, and joint procurement for the acquisition of advanced threat detection tools, as shown in ***Figure 6***. After a call for proposals in November 2022, ATHENA and ENSOC began their work in January 2024.

Figure 6 | Digital Europe Programme funding for cyber hubs



Source: ECA, based on ECCC data.

66 The two-phase restricted procurement procedures[11] were organised by the members of ATHENA and ENSOC, as well as DG Connect (the first phase) and the newly established ECCC (the second phase). The two-phase approach aims at limiting the circulation of sensitive information by providing the detailed technical specifications only to candidates selected in the first phase.

67 The first phase was launched in May 2024 for ENSOC and July 2024 for ATHENA. Interested companies had one month to apply. However, the successful candidates were only notified in April 2025, almost a year after the launch of the procedure.

68 In addition, neither the ENSOC nor the ATHENA procurement procedures could move on to the second phase at the time, as the hub members and the ECCC were unable to provide the shortlisted companies with the technical specifications necessary for them to submit an offer, since they were still working on finalising them.

[11] ENSOC call for tender and ATHENA call for tender.

69 The second phase of the procurement procedures only started in August 2025 for some ENSOC lots and was planned for early 2026 for ATHENA. At the time of the audit, 18 months after the launch of the procurement procedure, no contract had been signed for any of the lots. We consider that the lack of adequate preparation and the complexity of the procurement procedures were detrimental to their timely completion.

70 Therefore, we found that the cross-border hubs are not on track to achieve their objectives. Without the tools to detect threats and share information, they are operationally on hold and the European Cybersecurity Alert System is not yet functioning, delaying the effective development of advanced capabilities to detect and prevent cyber threats and incidents. Amendments have been signed to extend the duration of the grant agreement, to reflect the delays in the procurement procedures so far (15 months for ATHENA and 18 months for ENSOC).

Cross-border cyber hubs create additional communication channels that further increase complexity

71 One of the key tasks of the cross-border cyber hubs is to share relevant information to enhance threat detection and response. This includes information on cyber threats, vulnerabilities, indicators of compromise, and threat actors. The tasks of the cross-border cyber hubs partly overlap with those of the national CSIRTs and the CSIRTs network, especially regarding information sharing on cyber threats and vulnerabilities. There is no clear boundary between the roles of cross-border cyber hubs and CSIRTs. According to the 2025 Cyber Blueprint (paragraph ***29***), cross-border cyber hubs are meant to operate at both technical (such as the national CSIRTs and the CSIRTs network) and operational levels (such as EU-CyCLONe).

72 The Cyber Solidarity Act requires cross-border cyber hubs to sign cooperation agreements with one another to facilitate information sharing. ENISA should have issued guidelines for interoperability between cross-border cyber hubs by February 2026, as required by the Cyber Solidarity Act. In the meantime, in December 2025 the ECCC awarded a grant to a consortium (including certain ENSOC and ATHENA members) to define a technical framework for interoperability between cross-border cyber hubs. However, the guidelines and framework will only be completed once the cross-border cyber hubs are in operation. As we pointed out in our 2023 opinion on the proposal for the Cyber Solidarity Act[12], there

[12] Opinion 02/2023 concerning the proposal for a Regulation of the European Parliament and of the Council laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents, paragraph 26.

is a risk that, without a swift agreement, systems might be developed that are incompatible with one another, resulting in increased costs.

73 Cross-border cyber hubs are also required to share relevant information on large-scale cybersecurity incidents with EU-CyCLONe and the CSIRTs network without undue delay. At member-state level, the creation of national cyber hubs and participation in cross-border cyber hubs create additional layers of communication. The coordination with non-EU member states[13], which are not members of the CSIRTs network or EU-CyCLONe, also increases complexity.

74 Clear cooperation agreements are necessary to agree on a common taxonomy and on how to share information, and to ensure interoperability. Lessons learned from the CSIRTs network show that this is a significant challenge. We found that, at the time of the audit, no procedural arrangements on cooperation and information sharing had been agreed. We consider that establishing national and cross-border cyber-hubs could promote more effective information sharing. However, integrating the cross-border hubs into the already complex cybersecurity landscape will be challenging and requires additional communication channels and cooperation arrangements.

EU-funded projects under DIGITAL aim to strengthen cybersecurity, but face implementation and reporting challenges

Delays in its establishment prevented the Cybersecurity Competence Community from shaping DIGITAL according to its needs

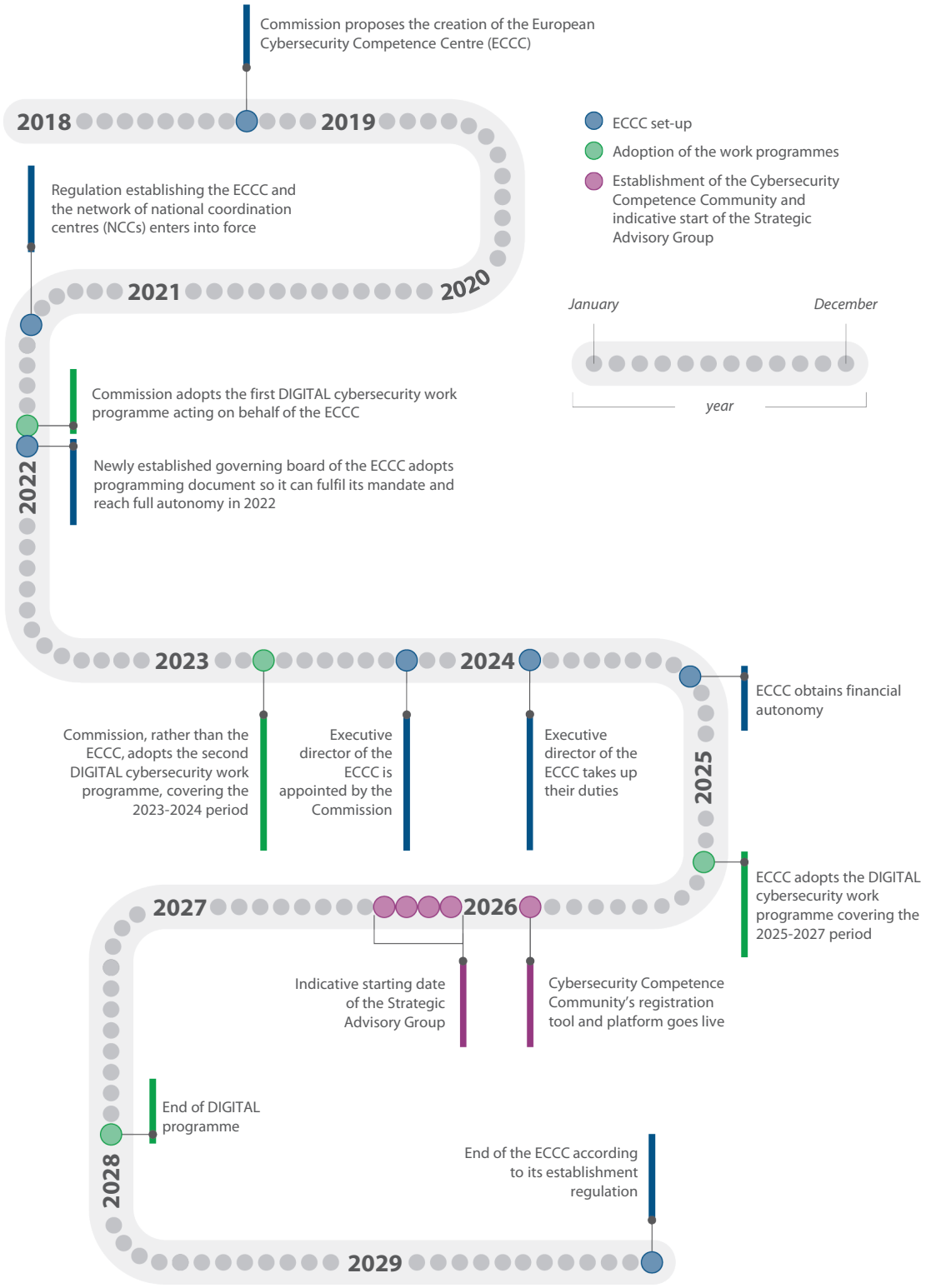
75 To manage the cybersecurity component of DIGITAL, in 2018 the Commission proposed the creation of the European Cybersecurity Competence Centre (ECCC). The ECCC Regulation planned for the ECCC to be supported by a network of 29 national coordination centres (NCCs), one for each member state, as well as Iceland and Norway. It also called for the creation of the Cybersecurity Competence Community (the Community), consisting of representatives of industry, academic, and research organisations, as well as other relevant civil society associations.

[13] Iceland and Norway.

76 Up to 20 members of the Community would be appointed to the Strategic Advisory Group (SAG), which is one of the three components of the ECCC's structure. One of the SAG's key tasks is to organise public consultations to feed the ECCC's agenda and DIGITAL work programmes.

77 We assessed whether DIGITAL and its work programmes were adopted on the basis of a sound analysis of needs, as well as how the ECCC, the Network of NCCs, the Community, and the SAG were able to contribute to the work programmes. In practice, the ECCC, the Network of NCCs, the Community, and the SAG have been set up gradually over several years (see ***Figure 7***).

Figure 7 | Timeline of the setting up of the European Cybersecurity Competence Centre, the network of national coordination centres, the Community, and the Strategic Advisory Group



Source: ECA.

78 Since the ECCC only became fully operational in September 2024, the Commission, on the ECCC's behalf, adopted the work programmes for the 2021-2022 and 2023-2024 periods. The two work programmes adopted by the Commission could not benefit from the input of the Community.

79 Meanwhile, member states began establishing their NCCs, which act as national-level points of contact for the Community. Their establishment and operation have been co-funded by DIGITAL, with over €90 million in EU funding granted by the time of the audit, including approximately €44 million that will be further distributed though financial support to third parties. An additional €38 million has been budgeted until 2027 to support NCCs.

80 We found that, in December 2025, four years after the establishment of the ECCC and the Network of NCCs, the Community had not yet been established, and the SAG had not yet been appointed. The ECCC adopted the latest DIGITAL cybersecurity work programme on 14 March 2025, covering the 2025-2027 period. While the ECCC prepared and adopted its work programme following extensive consultations with member states and the Network of NCCs, it could not benefit from input and advice from the Community or the SAG. This contradicts the provisions in its founding regulation and we consider this a missed opportunity.

81 DIGITAL is set to expire in 2027 and, if its mandate is not extended, the ECCC is expected to wind up in 2029. Therefore, the support of the network of NCCs, the Community, and the SAG, once in place, might only be relevant for a short period.

EU-funded projects pursue relevant objectives, but many face operational issues

82 We selected a sample of 11 projects relevant to the detection of and response to cybersecurity incidents and funded under DIGITAL in the 2022-2025 period (see ***Figure 5*** in ***Annex I*** and ***Annex III***). We assessed whether:

- the projects' objectives were in line with the expected outcomes expressed in the calls for proposals and those of DIGITAL overall;
- the projects have achieved their planned outputs and results so far;
- the projects' outputs have been delivered on time.

We present the outcome of this assessment in ***Annex IV***.

Some projects show early results but many face operational challenges and delays

83 We found that all projects pursue objectives that contribute to achieving the cybersecurity objectives of DIGITAL[14], and that they address most of the objectives of the calls for proposals[15].

84 Out of the 11 projects in our sample, two projects were at an early stage of implementation, and we therefore could not conclude on their performance. Of the remainder, we assessed four as satisfactory in terms of the achievement of their planned outputs and results. We considered that two projects show some weaknesses, and we assessed three as unsatisfactory (see ***Annex IV***).

85 DIGITAL explicitly aims to raise the cybersecurity level of small and medium-sized enterprises (SMEs). In that respect, several projects offer concrete solutions for SMEs (see ***Box 2***).

[14] Article 6 of Regulation (EU) 2021/694 establishing the Digital Europe Programme.

[15] Calls: Capacity building of security operation centres; Deploying the network of national coordination centres with member states; Preparedness support and mutual assistance; and Novel applications of AI and other enabling technologies for security operation centres.

Box 2

Examples of projects bringing tangible results to SMEs

The GR-SME-SOC project (project 6 in ***Annex III***) aims to provide cybersecurity tools and services to SMEs in Greece by establishing a security operations centre (SOC) tailored to their needs. The project started in January 2024 and is being implemented by a consortium of five Greek organisations. The plan is to offer cybersecurity services, free of charge, to 120 SMEs for one year, after which the services will become commercially available. The project offers SMEs advanced services such as real-time monitoring, AI-driven threat detection and agile incident response.

With the NCC-IE project (project 3 in ***Annex III***), the project coordinator provided around €1.8 million in grants to over 50 Irish SMEs to improve their cybersecurity. The grant scheme benefited companies with 2 to about 200 employees, including family businesses, start-ups, and global exporters in various sectors. The grants were exclusively for companies that had previously undergone a cyber security review managed by the government agency Enterprise Ireland. The grant covered 80 % of costs (up to €60 000) to implement the recommendations from the review.

Source: ECA.

86 Many projects in our sample are struggling to meet deadlines or are facing operational challenges (see ***Annex IV***). We found that four projects face considerable delays. This includes ENSOC and ATHENA, as detailed in paragraphs ***65***-***70***. We provide other examples in ***Box 3***.

Box 3

Examples of projects facing operational challenges and delays

In Ireland, the Local Government Management Authority (LGMA) is the sole beneficiary of the grant for the ILG-SOC project (project 8 in ***Annex III***). The project's objective is to set up a central security operations centre for 31 local authorities to use advanced threat detection and response tools. The project started in October 2023, with a duration of three years. The midterm review resulted in all deliverables being rejected. The project includes several procurement procedures which have failed or suffered delays. The duration of the project will be extended (without any additional funding), which could give the project enough time to conclude successfully.

In Greece, the EL-SOC project (project 5 in ***Annex III***) aims to set up a consolidated SOC at national level, which would bring together information from sectoral SOCs. This would provide a real-time and comprehensive overview of the cybersecurity situation. The project is running from January 2024 to December 2026. The planned procurement of hardware and services was delayed due to issues in finalising and

publishing the technical specifications for the call for tenders. As reasons for the delay, the project coordinator also mentioned issues related to securing national co-funding and the limited availability of procurement staff.

Source: ECA.

87 Two other projects in our sample face moderate delays. Three projects have been delivering their outputs on time. Finally, two projects are at an early stage of implementation and we therefore cannot reach a conclusion.

Security restrictions have led to operational challenges, and significant risks exist when checks are performed by beneficiaries

88 The DIGITAL Regulation provides that, for security reasons, funding for cybersecurity may be restricted to entities that are established in the EU and controlled by member states or EU citizens. This restriction aims to mitigate the risk of intrusion or influence by non-EU states and prevent sensitive security information from being shared with non-EU authorities.

89 The EU ownership and control obligation applies not only to grant beneficiaries but also to their subcontractors and any recipients of financial support to third parties (FSTP). Except for the latter category (see paragraphs ***92***-***96***), the Central Validation Service of the European Research Executive Agency performs the assessment. However, the final decision on the eligibility to participate in restricted calls is still up to the granting authority, i.e. DG Connect or the ECCC.

90 During our audit work, beneficiaries repeatedly mentioned the practical challenges posed by the ownership and control assessments (OCAs). Assessing EU ownership and control can be a complex and lengthy process. It requires analysing the complete ownership structure and chain of control of each organisation, including all ownership layers until the ultimate owners. The Central Validation Service requires that each entity provides extensive documentary evidence of their ownership structure and specific rights, corporate governance, and any commercial, financial, or other links conferring control.

91 In three EU-funded projects in our sample, at least one beneficiary of a consortium was later excluded because they were considered to be owned or controlled from outside the EU. The exclusion of consortium members shows that the notion of EU ownership and control is not fully understood by all DIGITAL participants. Overall, based on data from the Central Validation Service, 7 % of all DIGITAL cybersecurity grant applicants or sub-contractors have failed the assessment in the 2022-2025 period. The submission to a call for proposals of applications by ineligible participants causes delays, as illustrated in ***Box 4***.

Box 4

Example of a case where beneficiaries were excluded after failing the security checks

Two of the consortium members of the NG-SOC project (project 7 in ***Annex III***) failed the OCA. The outcome was announced around one month before the deadline for signing the grant agreement. The project coordinator had to agree to take over the work that had been assigned to the two excluded members, as there was no time to find a new partner. One of the excluded members was in a specific industry where the developed solution was to be piloted. Therefore, a significant part of the project, which concerned testing the solutions in practice, could not go ahead as intended. This situation was later remedied by amending the grant agreement to include new members.

Source: ECA.

92 Two of the projects we reviewed (NCC-IE and CYberSynchrony) provide financial support to third parties (FSTP). This funding mechanism enables grant beneficiaries to use some of the grant funding to fund other entities through open calls. FSTP can facilitate access to EU funding. In this case, the beneficiaries bear sole responsibility for conducting the OCAs, and the Central Validation Service is not involved.

93 In 2021, the Commission published general public guidance for applicants of restricted calls, updated in 2026. Although FSTP has been in place since 2021 for DIGITAL calls, neither the Commission nor the ECCC has provided a detailed methodology to beneficiaries on how to perform OCA checks when assessing the third parties to which they provide financial support. In July 2025, the ECCC shared non-mandatory guidance, providing the Network of NCCs with a structured approach to OCAs. The guidance document contains general principles and steps that could be taken. However, the guidance does not specify how the checks should be carried out, leaving beneficiaries responsible for developing their own approach.

94 We found that the ECCC neither validates the methodology adopted by the beneficiaries nor performs sample-based checks to ensure that the methodology is robust enough and that the selected recipients of financial support are indeed EU-owned and controlled.

95 In our 2024 annual report, we found that the beneficiaries entrusted by the Commission with the management of FSTP (in the area of research) were not required to demonstrate the effectiveness of their checks to ensure the regularity of the EU spending. Similarly, there is no assessment by the ECCC of the administrative and technical capacity of the beneficiaries to properly manage the OCAs. As detailed in paragraph ***90***, this assessment can be complex and is performed at EU level by a dedicated service with specialised expertise.

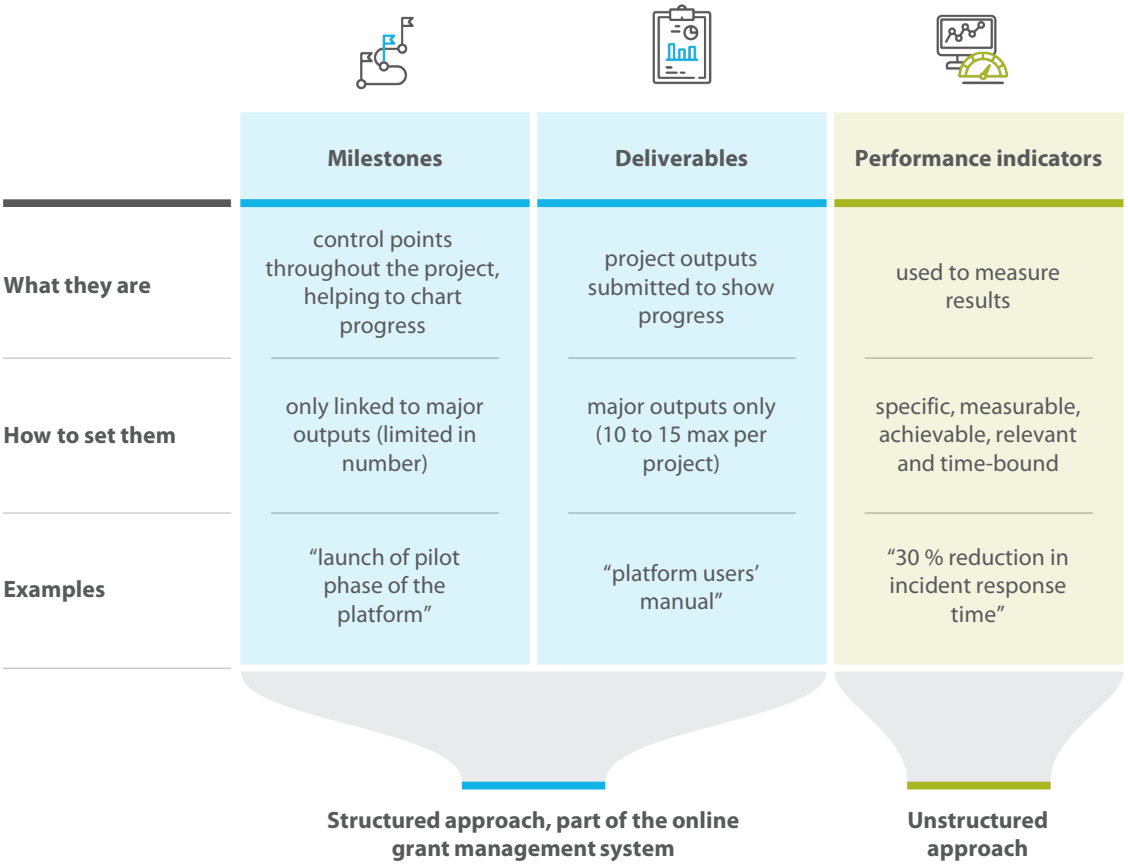
96 In this context, we consider that there is a significant risk that the beneficiaries, who are responsible for carrying out the OCA checks, do not have the capacity to perform them properly. Given the nature of the activities funded, this shortcoming could expose sensitive infrastructure, operational data, and security-critical technologies.

Most EU-funded projects have inadequate performance frameworks, and DIGITAL's cybersecurity-related performance data is not accurate

Most EU-funded projects have inadequate performance frameworks

97 Beneficiaries managing EU-funded projects must report on their progress and results to the ECCC using milestones, deliverables, and indicators, as illustrated in ***Figure 8***. We assessed whether the milestones and deliverables set for each project adequately allow for project monitoring. We also assessed whether their performance indicators are relevant and measurable, and have a baseline and a target.

Figure 8 | Milestones, deliverables, and performance indicators in DIGITAL projects



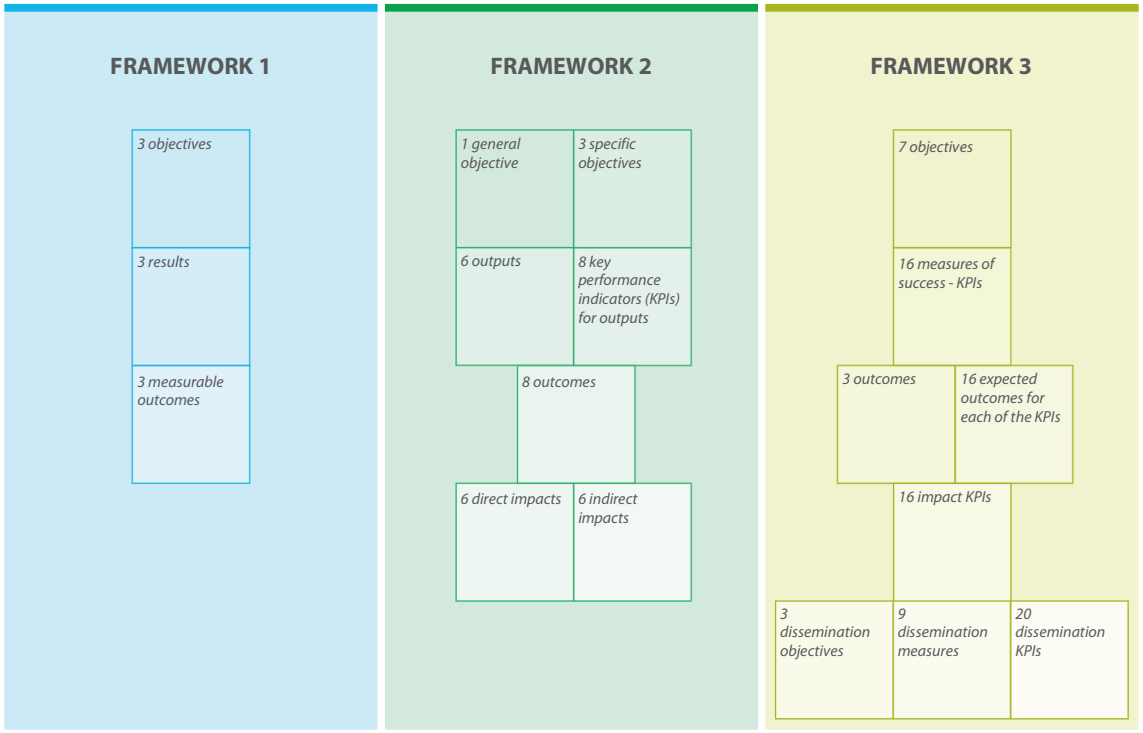
Source: ECA, based on the grant application form.

98 In their project proposal, beneficiaries must set a series of milestones and deliverables following a structured approach specified in the instructions to the applicants. All the milestones and deliverables are listed in the online grant management system to facilitate their follow-up. The ECCC usually reviews each project twice: once halfway through the project, and once after it is completed. During these reviews, external experts verify the achievement of milestones and deliverables, and the ECCC validates them. Milestones and deliverables are therefore key to project monitoring and should be set properly.

99 We found that almost none of the projects in our sample followed the instructions regarding the number of milestones and deliverables: the number of milestones per project varies from 8 to 39, while the number of deliverables ranges from 8 to 45. Many of the milestones and deliverables do not respect the instructions on how they should be drawn up and are therefore not useful for tracking progress (for example, “meeting to initiate drafting of research proposal call” or “formal project meeting minutes”). For three projects, the evaluation committee had identified these issues before grant signature. In two cases, the beneficiaries only proposed minor changes (e.g. to the due dates) without addressing the core issues, while the third one did not make any changes. For six other projects in our sample, our analysis shows that the milestones or deliverables are not in line with the instructions and are not always adequate. We consider that having poorly defined deliverables or milestones, or having too many, makes tracking progress difficult.

100 Contrary to the milestones and deliverables, performance indicators do not follow a structured approach and are not consolidated in a table in the grant management system, but instead can be found throughout different sections of the proposal. This approach has resulted in a plethora of performance frameworks being proposed by the beneficiaries. While some have only set project objectives linked to performance indicators, others have set up far more complex performance frameworks. We provide some examples in ***Figure 9*** below.

Figure 9 | Example of the variety of performance frameworks designed for the projects



Source: ECA.

101 Our analysis concludes that many of the performance indicators used by the projects are not relevant or measurable, and lack a target or a baseline (see ***Box 5***). Moreover, seven projects have defined 20 or more indicators, with one project having 52. We present the outcome of this assessment in ***Annex IV.***

Box 5

Examples of inadequate performance indicators

Not measurable:

- "Indicator of compromise and other provided services strengthen SMEs' cybersecurity capacities"
- "Delivery of incident response tools and methods enabling integration with EU-CyCLONe communication channels"

Not provided with a baseline or a target:

- "≥ 20 % improvement in preparedness of staff"

- "≥ 20 % reduction in effort required to align and comply with relevant EU cybersecurity initiatives"

Not performance-related:

- "Final report on project at end of funding phase"
- "Number of trainees who will participate in all training sessions"

Source: ECA, based on project documentation.

102 Overall, we consider that the wide variety of performance frameworks, the poor set-up of the indicators and their excessive number complicate performance monitoring significantly. It is therefore not possible to assess project performance properly. This is further complicated by the fact that the reporting template does not contain a dedicated section on projects' performance indicators and, as a result, most projects in our sample did not report on them.

Performance data on the cybersecurity component of DIGITAL is not accurate

103 To monitor the achievements of DIGITAL, the Regulation provides programme indicators on which all projects must report, as detailed in ***Box 6***.

Box 6

DIGITAL indicators for cybersecurity

1.a The number of cybersecurity infrastructure, or tools, or both jointly procured, including in the context of the European Cybersecurity Alert System

1.b The number of cybersecurity infrastructure, or tools, or both deployed

2. The number of users and user communities getting access to European cybersecurity facilities

3. The number of actions supporting preparedness for and response to cybersecurity incidents under the Cybersecurity Emergency Mechanism

Source: Annex II to Regulation (EU) 2021/694 establishing the Digital Europe Programme; the monitoring and evaluation framework for the Digital Europe Programme (SWD(2024) 37).

104 We assessed whether the projects in our sample had reported on these indicators and examined how the ECCC collects and verifies this data.

105 All projects are requested to report on the DIGITAL indicators prior to their midterm and final reviews in the grant management system. We found that, out of seven projects that were halfway through their timeline during our audit and that should therefore have reported on these indicators, only three had done so. Out of these three, two had not reported accurate information: one reported on the wrong indicator, the other one provided target values instead of achieved results.

106 Each year, the Commission reports on these indicators in its programme performance statements. This enables stakeholders to assess whether the programme is delivering on its objectives. According to the 2024 programme performance statements, the DIGITAL indicators for cybersecurity are on track. The ECCC has explained to us that it used a series of surveys sent to project beneficiaries to compile these indicators, rather than basing them on the grant management system. We reviewed the disaggregated data provided by the ECCC and found numerous issues in the way data was collected and its overall quality. We found that the data collected does not match the values presented in the programme performance statement, so it is unclear how the reported values have been calculated. We found no evidence that the accuracy of the reported data was verified by the ECCC. Based on our checks of the projects in our sample, as most values are missing or inaccurate, we consider that the reported data does not properly reflect the achieved results.

This report was adopted by Chamber III, headed by Mr George-Marius Hyzler, Member of the Court of Auditors, in Luxembourg at its meeting of 16 June 2026.

For the Court of Auditors

Tony Murphy
President

Annexes

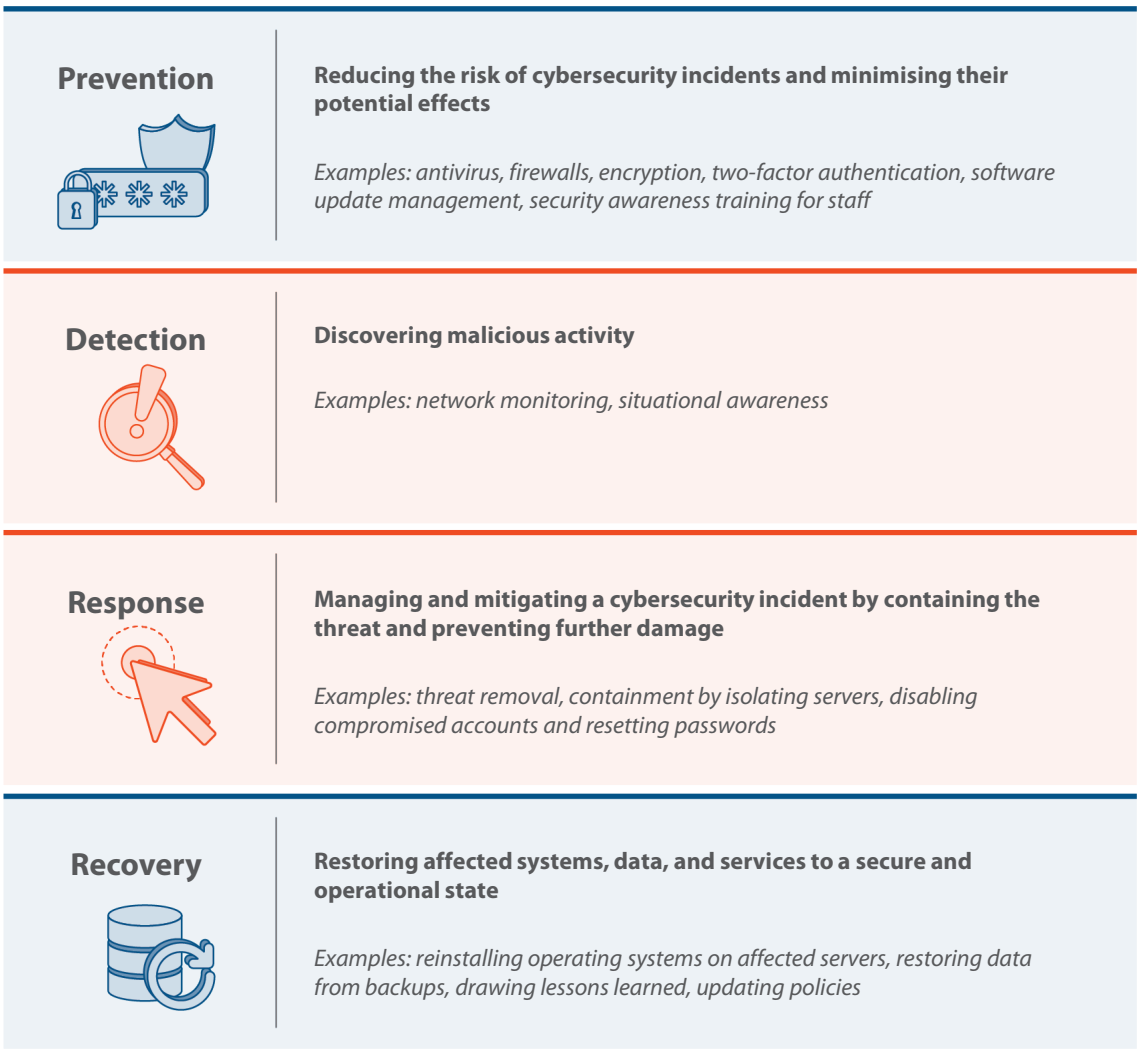
Annex I – About the audit

01 Cybersecurity is defined as "the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats"[1]. A cyber threat is "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons"[2]. Cybersecurity requires a holistic approach, consisting of a series of interrelated activities to prevent, detect, respond to, and recover from cyber threats, as shown in ***Figure 1*** below.

[1] Regulation (EU) 2019/881 (Cybersecurity Act).

[2] Article 2 of the Cybersecurity Act.

Figure 1 | Examples of cybersecurity activities

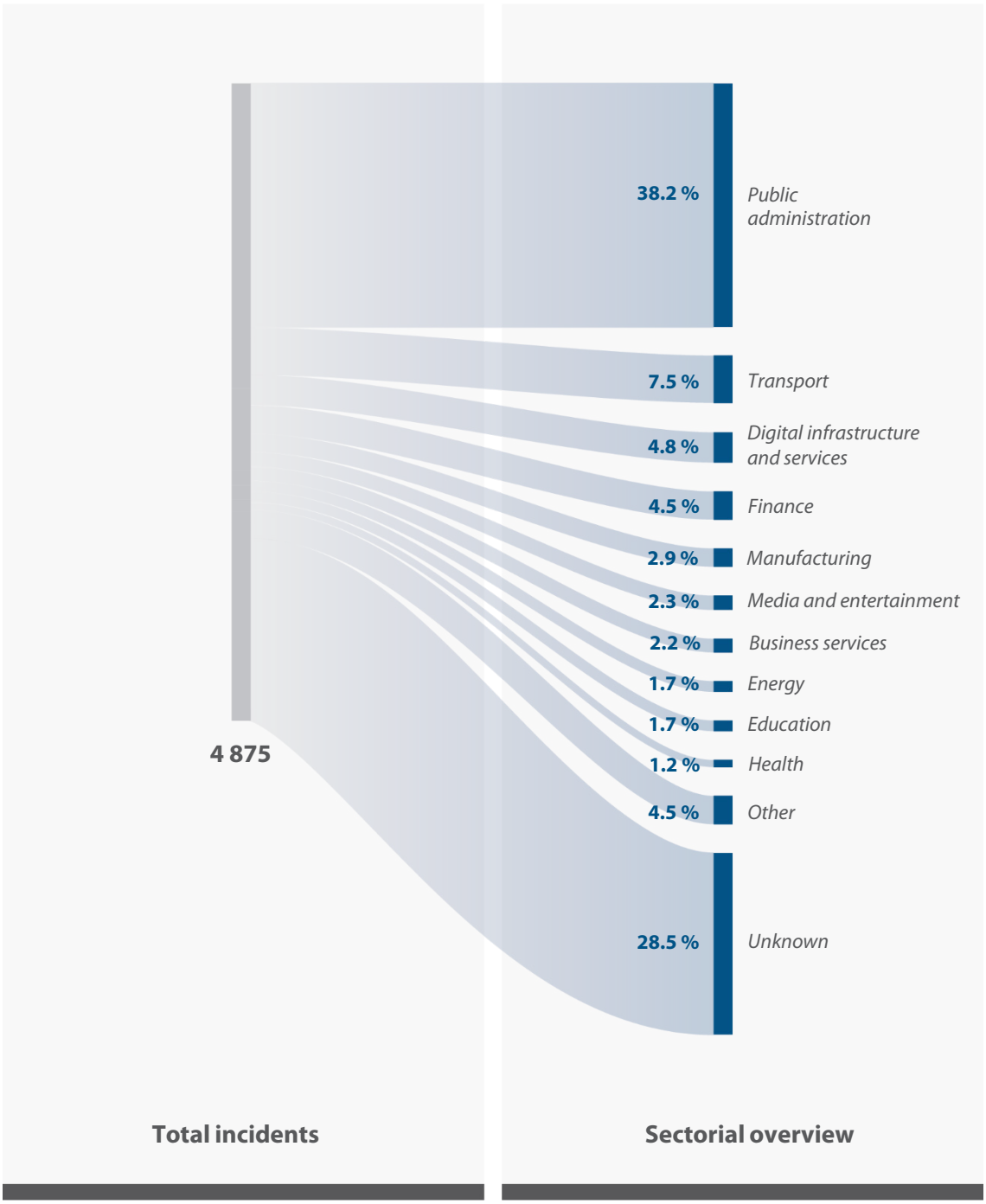


Source: ECA, based on recital 78 to Directive (EU) 2022/2555 on measures for a high common level of cybersecurity (NIS 2 Directive).

02 The European Union Agency for Cybersecurity (ENISA) considers the cybersecurity threat level to be substantial, while noting that the cybersecurity threat landscape has become and continues to be significantly more complex[3]. These threats underline the vital importance of cybersecurity in increasingly digital economies and societies. In its 2025 threat landscape report, ENISA identified ransomware as the most critical threat in the EU. ***Figure 2*** shows the targeted sectors.

[3] ENISA's 2024 report on the state of cybersecurity in the Union.

Figure 2 | Sectors targeted by cyber attacks



Source: ECA, based on ENISA.

Significant and large-scale cybersecurity incidents

03 Cybersecurity incidents, which include cyber threats and unintentional events (such as those mentioned in ***Figure 3*** and paragraph ***40***), "can impede the provision of public services [and] the pursuit of economic activities,… generate substantial financial losses, undermine user confidence, cause major damage to the economy and the democratic systems of the Union, and could even have health or life-threatening consequences"[4]. A cybersecurity incident is considered[5]:

- **significant**, if it has caused or could cause severe operational disruption to the services or financial loss to the entity concerned, or if it has affected or could affect other natural or legal persons by causing considerable material or non-material damage;
- **large-scale**, if it has caused a level of disruption that exceeds a member state's capacity to respond or that significantly affects at least two member states.

04 A large-scale cybersecurity incident may escalate into a fully fledged **EU cyber crisis** if it prevents the proper functioning of the internal market or poses serious public security and safety risks for entities or citizens in several member states, or the EU as a whole[6].

EU policy framework

05 The EU's cyber ecosystem is complex and multilayered, and cuts across an array of internal policy areas, such as justice and home affairs, the digital single market, and research policies[7]. In external policy, cybersecurity features in diplomacy and is increasingly part of the EU's emerging defence policy[8].

06 In recent years, the EU has reinforced its cybersecurity regulatory framework. ***Figure 3*** below presents the most relevant legislation and policy instruments at EU level. In line with

---

[4] Recital 2 to Regulation (EU) 2025/38 (the Cyber Solidarity Act).

[5] Articles 6 and 23 of the NIS 2 Directive, further specified in Commission Implementing Regulation (EU) 2024/2690 for a number of providers in the digital infrastructure sector.

[6] Recital 69 to the NIS 2 Directive.

[7] ECA briefing paper on challenges to effective EU cybersecurity policy, p. 12.

[8] For example, the European Union's cyber posture (2022), the framework for a coordinated EU response to hybrid campaigns (2022), the EU policy on cyber defence (2023), and the revised cyber diplomacy toolbox (2023).

our audit scope (see paragraphs *13-14*), we have focused on instruments dealing with the detection of and response to significant and large-scale cybersecurity incidents.

Figure 3 | Relevant EU legislation and policy instruments

Source: ECA.

Roles and responsibilities

07 The EU cybersecurity landscape involves numerous private and public entities at regional, national and EU level in the civilian sphere, including law enforcement. Cybersecurity is also a key element of national security and defence[9]. We illustrate the current EU landscape in ***Annex II***.

08 Member states bear primary responsibility for preventing, preparing for, and responding to any cybersecurity incidents and crises that affect them. In accordance with Article 4(2) of the Treaty on European Union, national security remains the sole responsibility of each member state. As cybersecurity incidents could disrupt and damage critical information infrastructure, on which the smooth functioning of the internal market depends, the EU also plays an important role in the event of a significant incident or crisis[10]. The main entities at EU level are presented in ***Figure 4*** below.

[9] Opinion 02/2023 on the proposed Cyber Solidarity Act.

[10] EU blueprint for cyber crisis management.

Figure 4 | Entities at EU level with a key role in cybersecurity

Source: ECA.

EU funding

09 Under the current 2021-2027 multiannual financial framework, the main source of funding for cybersecurity is the Digital Europe Programme (DIGITAL). Launched in 2021, it is the first EU programme that specifically aims to drive the digital transformation of the EU, and it has a total budget of €8.1 billion[11].

[11] Digital Europe Programme.

10 DIGITAL funds cybersecurity actions under its specific objective 3 – "Cybersecurity and trust". More precisely, there is a budget of €1.4 billion for:

- strengthening cybersecurity coordination between member states' tools and data infrastructure;
- supporting the wide deployment of the cybersecurity solutions across the economy.

11 Most of the DIGITAL funding for cybersecurity is provided through calls for proposals, with 12 calls launched between November 2021 and December 2025. The available EU funding for these calls amounts to €825 million. New calls are planned for 2026 and 2027, to award a further €212 million in grants.

12 Another significant EU programme supporting cybersecurity is Horizon Europe. Cybersecurity projects are mainly funded under cluster 3 – "Civil security for society" – and are usually at an early stage of maturity due to Horizon Europe's focus on research and innovation. The Recovery and Resilience Facility also provides funding for cybersecurity measures.

Audit scope and approach

13 The increase of cyber threats and their potential impact have highlighted the need to strengthen our collective cyber resilience. The objective of our audit was to assess whether EU actions facilitate the detection of and response to significant and large-scale cybersecurity incidents effectively. In particular, we assessed whether this was the case for:

- EU-level networks and mechanisms (namely, the CSIRTs network, EU-CyCLONe, the European Cybersecurity Alert System, the cyber situation centre, and the EU Cybersecurity Reserve);
- actions funded under DIGITAL.

We did not cover EU-level law enforcement cooperation, nor cyber deterrence actions undertaken at EU level through diplomatic measures or defence activities.

14 The audit covers the period from 2022 to 2025. It is based on a desk review and analysis of relevant documents, audit visits to three member states (Ireland, Greece and Italy), and written questionnaires and interviews with relevant stakeholders. ***Figure 5*** shows how we obtained evidence for our observations.

Figure 5 | Audit work carried out

We examined

- The **legal framework** applicable to the detection of and response to significant and large-scale cybersecurity incidents
- The **roles and responsibilities** of networks and structures set up at EU level

We analysed

- Documents on the functioning of the **CSIRTs network** and **EU-CyCLONe**
- Documentation on the **DIGITAL programming and performance monitoring framework**
- Documentation on **13 selected EU-funded actions** (11 grants and 2 contracts – see detailed list in Annex III)

* We have selected EU-funded actions in three countries (Ireland, Greece, and Italy) where the relevant DIGITAL funding was more material. The 11 grants were drawn from a list of 137 EU-funded projects relevant to threat detection and response, with a view to cover a diverse mix of projects.

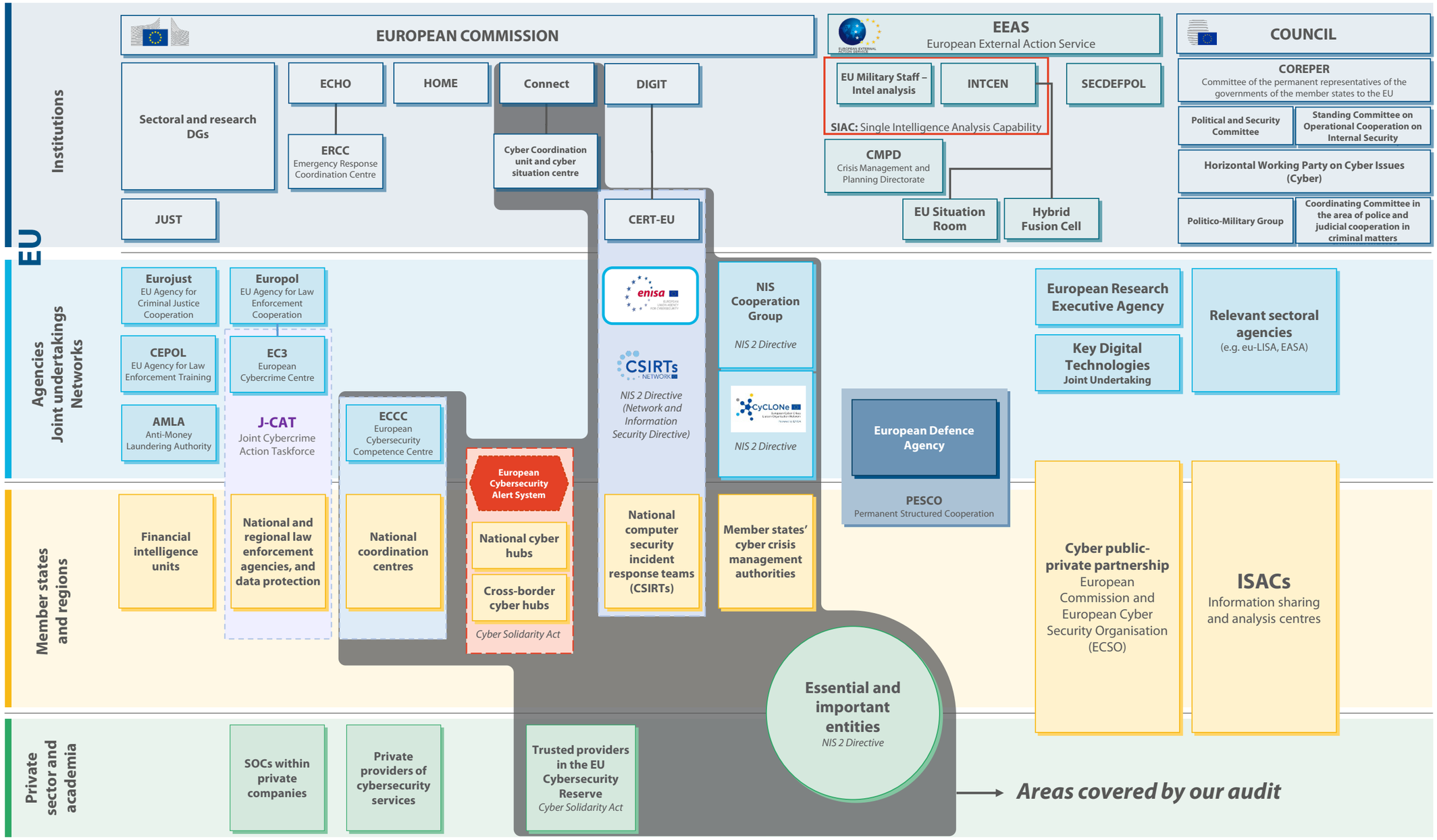
We interviewed

- Beneficiaries of the **11 sampled EU-funded grants**
- Representatives of the national cybersecurity authorities in **three members states** (Ireland, Greece, and Italy)
- Representatives of the European Commission (**DG Connect**), **ENISA**, and the **ECCC**

Source: ECA.

15 We expect our findings to contribute to improving the effectiveness and efficiency of the EU's detection of and response to significant and large-scale cybersecurity incidents, as well as improving the way EU-funded actions are selected and monitored. Our audit methodology complies with the international standards on auditing issued by the International Organization of Supreme Audit Institutions (INTOSAI).

Annex II – The EU cybersecurity landscape



DG Connect: Directorate-General for Communications Networks, Content and Technology
DG ECHO: Directorate-General for European Civil Protection and Humanitarian Aid Operations
DG HOME: Directorate-General Migration and Home Affairs
DG JUST: Directorate-General Justice and Consumers
DIGIT: Directorate-General for Digital Services
EASA: European Union Aviation Safety Agency
EU-CyCLONe: European Cyber Crisis Liaison Organisation Network
eu-LISA: European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice
INTCEN: European Union Intelligence and Situation Centre
SECDEFPOL: Security and Defence Policy
SOC: Security operations centre

Annex III – Selected cybersecurity actions

ID	Title	Countries	Start date	End date	Total cost (in million euros) and EU contribution (as %)	Link to EU Funding & Tenders Portal
Grants for cross-border cyber hubs that are part of the European Cybersecurity Alert System						
1	**Establishing Cross-border SOCs (ATHENA)**	Bulgaria, Greece, Cyprus, Malta	1.1.2024	31.3.2028	4.7 (50 %)	
2	**ENSOC-CROSSBORDER PLATFORM (ENSOC)**	Spain, Italy, Luxembourg, Netherlands, Austria, Portugal, Romania	1.1.2024	30.6.2028	10.4 (50 %)	
Grants for deploying the network of national coordination centres (NCCs) in member states						
3	**Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE)**	Ireland	2.10.2023	1.10.2026	4.2 (47 %)	
4	**Italian National Coordination Centre (NCC-IT)**	Italy	1.11.2023	31.10.2025	2.0 (50 %)	
Grants to build the capacity of security operations centres (SOCs), promote novel applications of AI and other enabling technologies for SOCs, and provide preparedness support and mutual assistance						
5	**Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)**	Greece, Cyprus	1.1.2024	31.12.2026	9.7 (50 %)	
6	**Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)**	Greece	1.1.2024	31.12.2026	12.1 (50 %)	

ID	Title	Countries	Start date	End date	Total cost (in million euros) and EU contribution (as %)	Link to EU Funding & Tenders Portal
7	**Next Generation Security Operation Centres (NG-SOC)**	Greece, Spain, Cyprus, Luxembourg, Slovenia, Norway	1.1.2024	31.12.2026	4.8 (50 %)	
8	**Irish Local Government Security Operations Centre (ILG-SOC)**	Ireland	1.10.2023	30.9.2026	8.3 (50 %)	
9	**An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)**	Ireland	1.1.2024	31.12.2026	3.6 (50 %)	
10	**Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)**	Belgium, Greece, Italy, Cyprus, Netherlands	1.6.2024	31.5.2027	7.0 (100 %)	
11	**Advanced Cooperative Security Operation Centres (ACSOC)**	Greece, Italy, Romania	1.1.2025	31.12.2027	3.0 (50 %)	
Framework contract for ENISA's Cybersecurity Support Action						
12	**Supporting ENISA for the Provision of Services under the Cybersecurity Support Action (28 lots)**	27 member-state lots 1 pan-European lot	1.12.2022[1]	31.12.2025	28.3 (100 %)	
Service contract for DG Connect's cyber situation centre						
13	**Bespoke Service to Support the Cyber Situation and Analysis Centre for the European Commission**	-	30.12.2022	30.12.2026	18.0 (100 %)	

Source: ECA.

[1] Multiple contracts signed throughout December 2022.

Annex IV – ECA assessment of EU-funded cybersecurity projects

Satisfactory *Some weaknesses*
Unsatisfactory *Not possible to conclude (too early to call)*

ID	Project	The project addresses most of the needs identified in the call	The project has achieved its planned outputs and results so far	The project's outputs have been delivered by their due date	Project's performance indicators are relevant, measurable and have a baseline and a target
1	Establishing Cross-border SOCs (ATHENA)	Satisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory
2	ENSOC-CROSSBORDER PLATFORM (ENSOC)	Satisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory
3	Development and Implementation of the National Cyber Security Coordination and Development Centre for Ireland (NCC-IE)	Satisfactory	Satisfactory	Some weaknesses	Some weaknesses
4	Italian National Coordination Centre (NCC-IT)	Satisfactory	Satisfactory	Satisfactory	Some weaknesses
5	Enhancing the capacity of the Hellenic Consolidated Security Operation Center (EL-SOC)	Satisfactory	Some weaknesses	Unsatisfactory	Unsatisfactory
6	Greek Security Operations Centre for Small and Medium Enterprises (GR-SME-SOC)	Satisfactory	Satisfactory	Satisfactory	Some weaknesses
7	Next Generation Security Operation Centres (NG-SOC)	Satisfactory	Satisfactory	Satisfactory	Some weaknesses
8	Irish Local Government Security Operations Centre (ILG-SOC)	Satisfactory	Unsatisfactory	Unsatisfactory	Unsatisfactory
9	An Interconnected Ecosystem of Cyber Security Coordination and Response Networks (Cyber-CORE-Network)	Satisfactory	Some weaknesses	Some weaknesses	Some weaknesses
10	Harmonizing People, Processes, and Technology for Robust Cybersecurity (CYberSynchrony)	Some weaknesses	Not possible to conclude (too early to call)	Not possible to conclude (too early to call)	Some weaknesses
11	Advanced Cooperative Security Operation Centres (ACSOC)	Satisfactory	Not possible to conclude (too early to call)	Not possible to conclude (too early to call)	Unsatisfactory

Abbreviations

Abbreviation	Definition/Explanation
CSIRT	Computer security incident response team
DG Connect	Directorate-General for Communications Networks, Content and Technology
DIGITAL	Digital Europe Programme
ECCC	European Cybersecurity Competence Centre
ENISA	European Union Agency for Cybersecurity
EU-CyCLONe	European Cyber Crisis Liaison Organisation Network
FSTP	Financial support to third parties
NCC	National coordination centre
NIS	Network and information security
OCA	Ownership and control assessment
SAG	Strategic Advisory Group
SME	Small or medium-sized enterprise
SOC	Security operations centre

Glossary

Term	Definition/Explanation
Cyber hub	Central platform bringing together various services, tools, and IT professionals to enhance the monitoring, detection and analysis of cyber threats, prevent cybersecurity incidents and support the production of cyber threat intelligence.
Cyber threat	Potential use of cyberspace to compromise the availability, authenticity, integrity or confidentiality of data or information systems.
Cybersecurity incident	Event compromising the availability, authenticity, integrity or confidentiality of data or information systems.
Large-scale cybersecurity incident	Cybersecurity incident that is too disruptive for a member state to handle alone or which has a significant impact on at least two member states.
Ransomware	Malware that denies victims access to a computer system or encrypts files to make them unreadable, usually forcing the victim to pay a ransom to restore access.
Security operations centre	Organisational unit that works to prevent cyber threats and incidents and gathers related intelligence.
Significant cybersecurity incident	Cybersecurity incident that has caused or may cause severe disruption or financial loss for an organisation, or considerable damage for other entities or individuals.
Taxonomy	In the context of cybersecurity, a classification scheme used to organise, categorise and structure knowledge about key concepts such as threats and incidents.
Threat actor	Individual or group intentionally causing harm, disrupting services or stealing data by exploiting vulnerabilities in IT systems, networks and devices.

Replies of the Commission

https://www.eca.europa.eu/en/publications/SR-2026-19

Replies of the European Cybersecurity Competence Centre (ECCC)

https://www.eca.europa.eu/en/publications/SR-2026-19

Replies of the European Union Agency for Cybersecurity (ENISA)

https://www.eca.europa.eu/en/publications/SR-2026-19

Timeline

https://www.eca.europa.eu/en/publications/SR-2026-19

Audit team

The ECA's special reports set out the results of its audits of EU policies and programmes, or of management-related topics from specific budgetary areas. The ECA selects and designs these audit tasks to be of maximum impact by considering the risks to performance or compliance, the level of income or spending involved, forthcoming developments and political and public interest.

This performance audit was carried out by Audit Chamber III – External action, security and justice, headed by ECA Member George-Marius Hyzler. The audit was led by ECA Member George-Marius Hyzler, supported by Romuald Kayibanda, Head of Private Office and Annette Farrugia, Private Office Attaché; Cyril Messein, Principal Manager; Frédéric Soblet, Head of Task; Jurgen Manjé and Flavia Di Marco, Auditors. Zoe Amador Martínez provided linguistic support. Dunja Weibel provided graphical support.

From left to right: Frédéric Soblet, Romuald Kayibanda, George-Marius Hyzler, Jurgen Manjé, Cyril Messein.

COPYRIGHT

HTML	ISBN 978-92-849-7859-5	ISSN 1977-5679	doi:10.2865/0019829	QJ-01-26-032-EN-Q
PDF	ISBN 978-92-849-7860-1	ISSN 1977-5679	doi:10.2865/6235204	QJ-01-26-032-EN-N

HOW TO CITE

European Court of Auditors, special report 19/2026 “Detecting and responding to cybersecurity incidents – EU cooperation framework progressing, but only partially effective due to implementation delays and limited information sharing”, Publications Office of the European Union, 2026.

In recent years, the EU has reinforced its cybersecurity regulatory framework and established networks and mechanisms to deal with cybersecurity incidents. The EU also funds cybersecurity projects through the Digital Europe Programme.

We conclude that EU actions only partially facilitate the detection of and response to significant and large-scale cybersecurity incidents. While a cooperation framework has gradually been put in place, work is still ongoing towards achieving full set-up. Limited information sharing, reporting weaknesses and considerable implementation delays prevent EU networks and mechanisms from reaching their full potential. Projects pursue relevant objectives, but several face operational challenges and delays. Moreover, there are weaknesses in the overall performance monitoring framework. We put forward recommendations to address these shortcomings.

ECA special report pursuant to Article 287(4), second subparagraph, TFEU.

EUROPEAN COURT OF AUDITORS

Publications Office of the European Union

EUROPEAN COURT OF AUDITORS
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Tel. +352 4398-1

Enquiries: eca.europa.eu/en/contact
Website: eca.europa.eu
Social media: @EUauditors